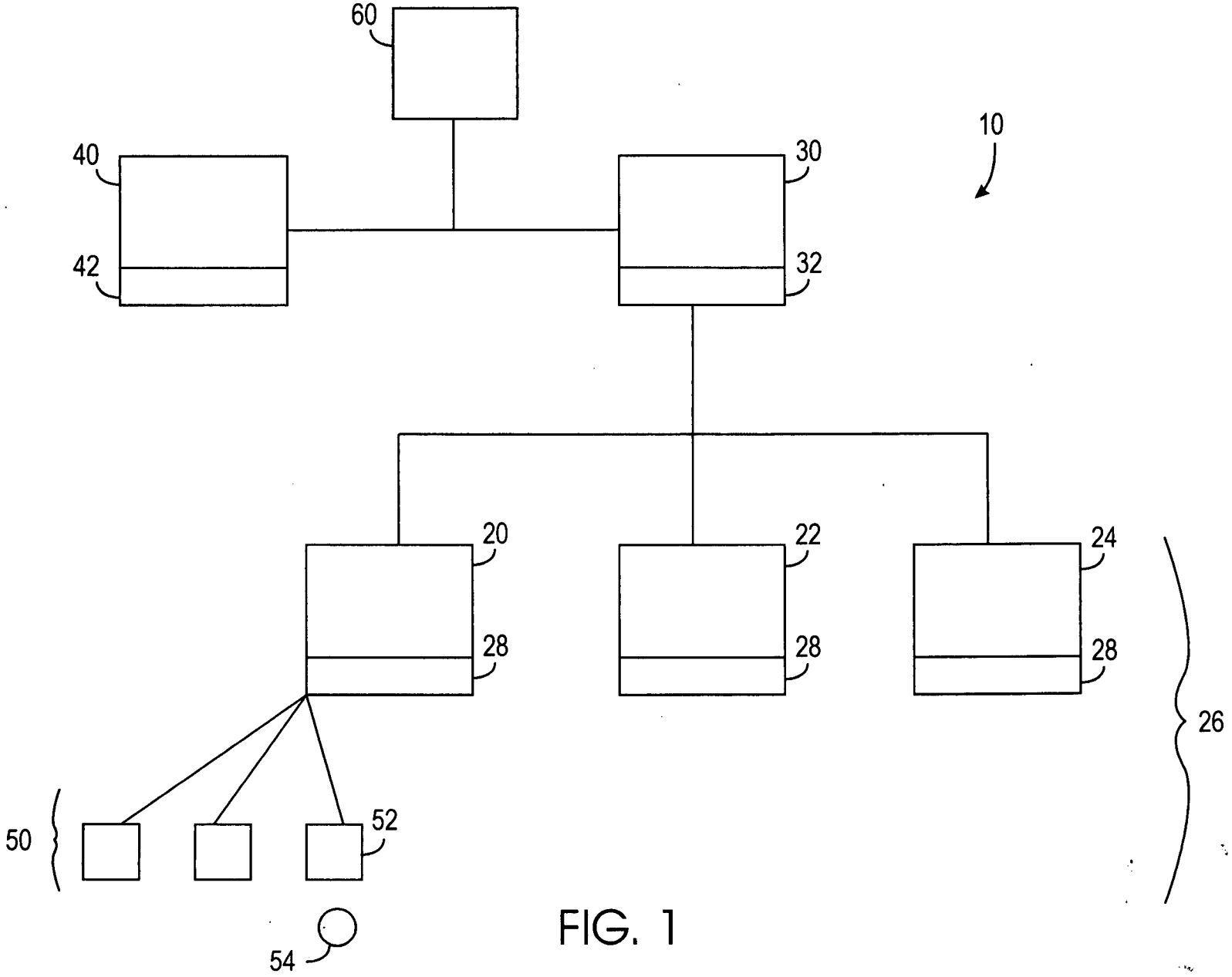



FIG. 1

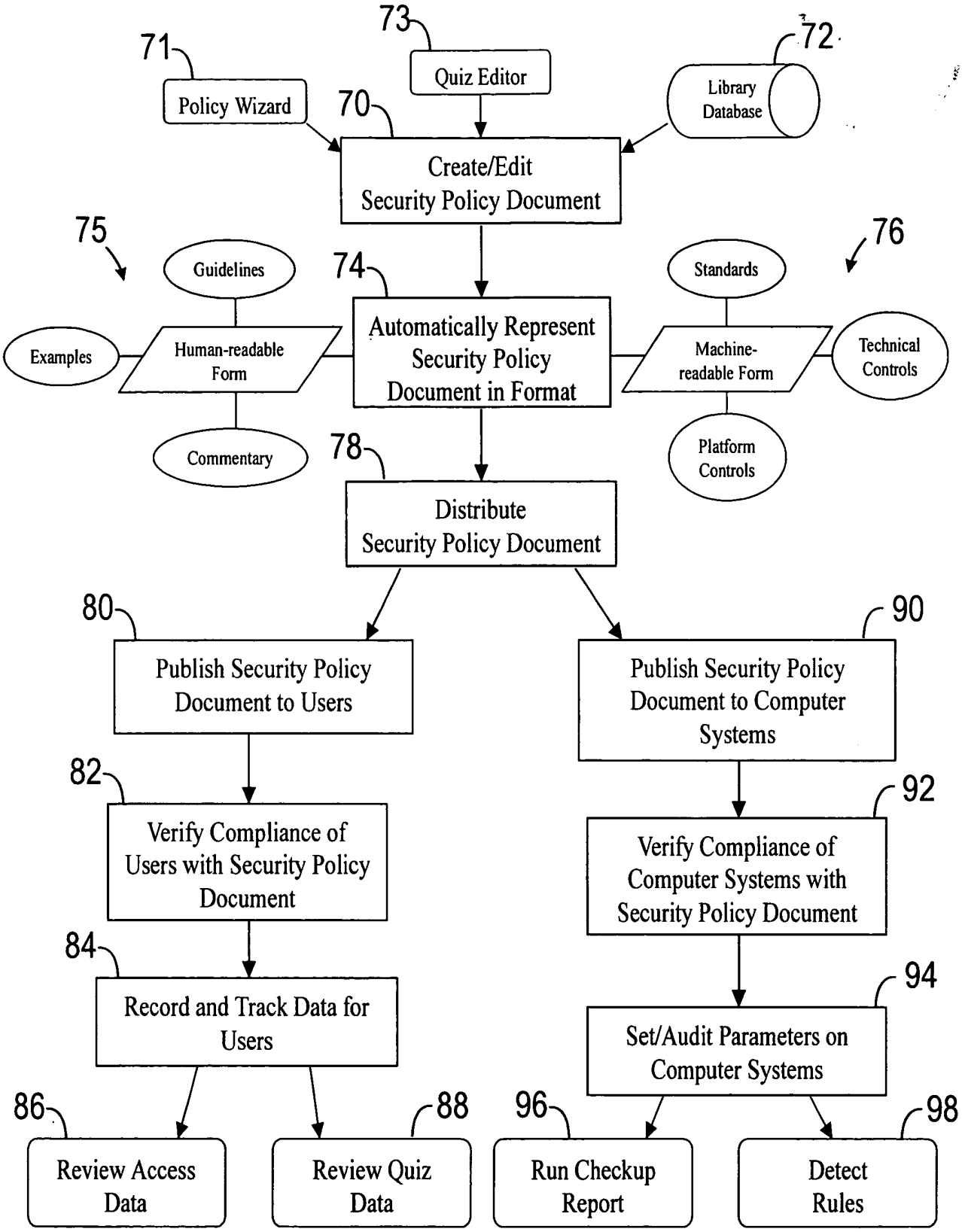

71
Policy Wizard
73
Quiz Editor
72
Library Database
70
Create/Edit Security Policy Document
75
Guidelines
74
Automatically Represent Security Policy Document in Format
76
Standards
Examples
Human-readable Form
Machine-readable Form
Technical Controls
Commentary
Platform Controls
78
Distribute Security Policy Document
80
Publish Security Policy Document to Users
90
Publish Security Policy Document to Computer Systems
82
Verify Compliance of Users with Security Policy Document
92
Verify Compliance of Computer Systems with Security Policy Document
84
Record and Track Data for Users
94
Set/Audit Parameters on Computer Systems
86
Review Access Data
88
Review Quiz Data
96
Run Checkup Report
98
Detect Rules

FIG. 2

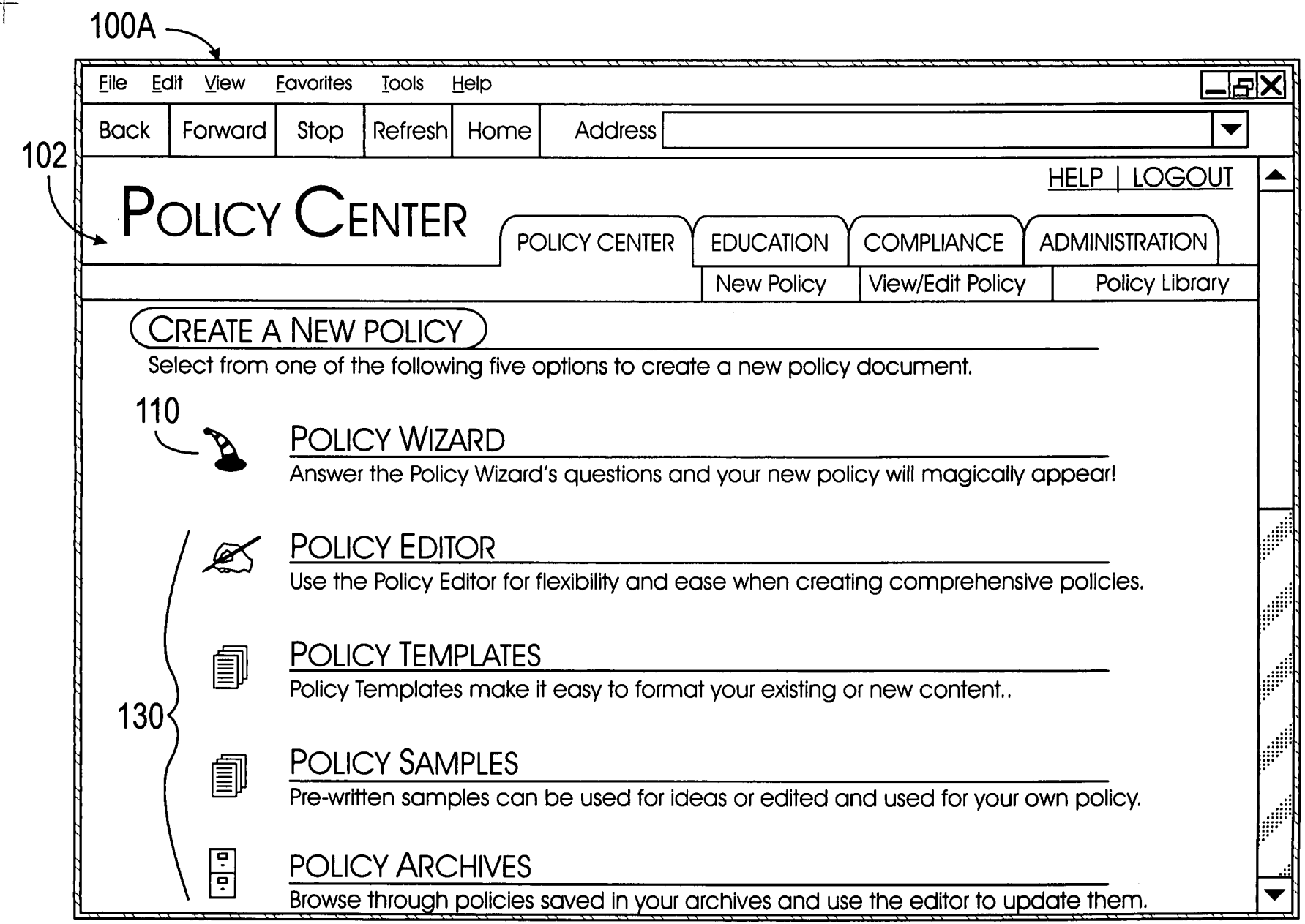

100A
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
102
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Policy View/Edit Policy Policy Library
CREATE A NEW POLICY
Select from one of the following five options to create a new policy document.
110
POLICY WIZARD
Answer the Policy Wizard's questions and your new policy will magically appear!
POLICY EDITOR
Use the Policy Editor for flexibility and ease when creating comprehensive policies.
POLICY TEMPLATES
Policy Templates make it easy to format your existing or new content..
130
POLICY SAMPLES
Pre-written samples can be used for ideas or edited and used for your own policy.
POLICY ARCHIVES
Browse through policies saved in your archives and use the editor to update them.

FIG. 3

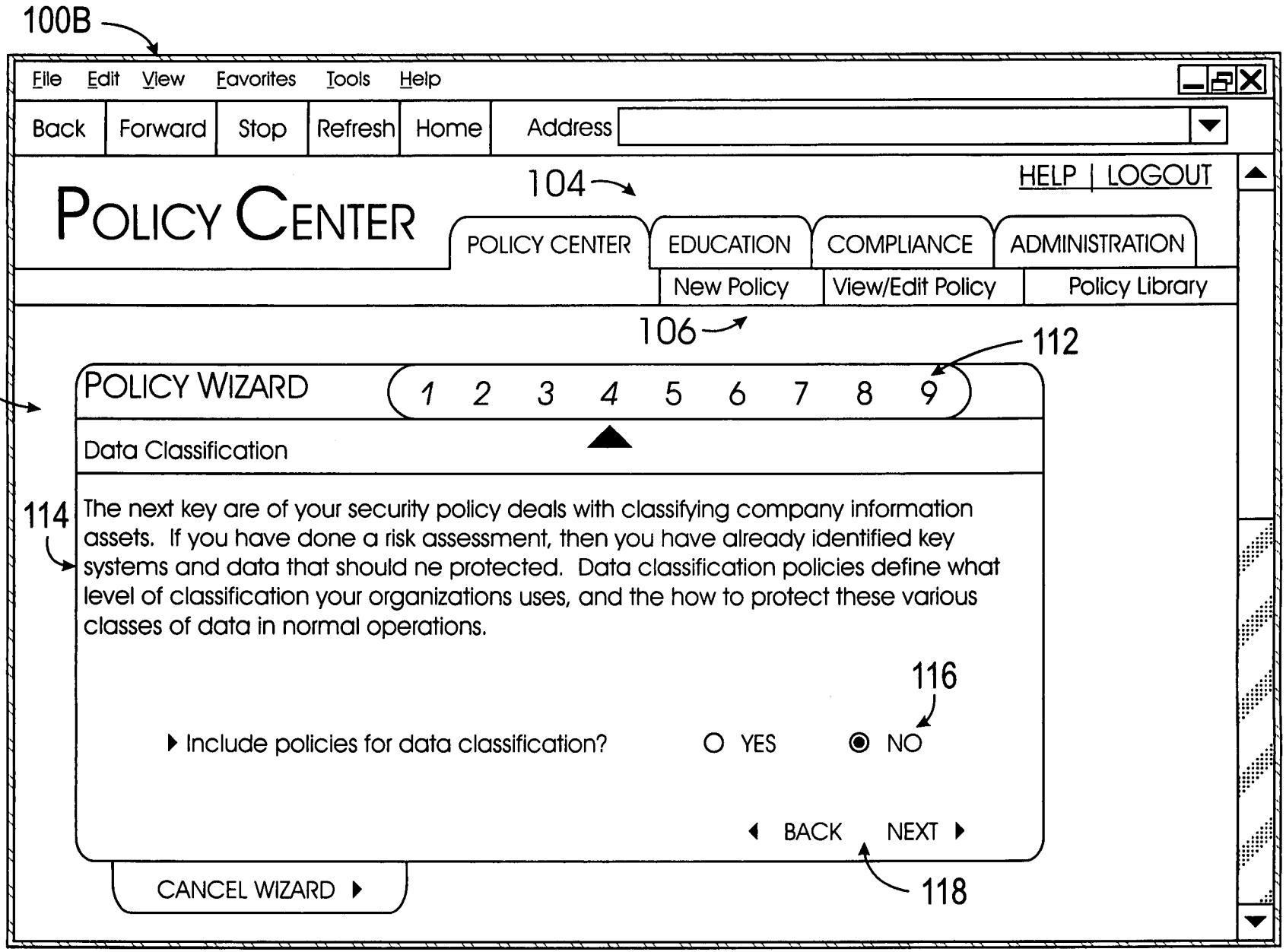

100B
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
HELP | LOGOUT
POLICY CENTER
104
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Policy View/Edit Policy Policy Library
106
110
112
POLICY WIZARD
1 2 3 4 5 6 7 8 9
Data Classification
114
The next key are of your security policy deals with classifying company information assets. If you have done a risk assessment, then you have already identified key systems and data that should ne protected. Data classification policies define what level of classification your organizations uses, and the how to protect these various classes of data in normal operations.
116
Include policies for data classification? YES NO
BACK NEXT
CANCEL WIZARD
118

FIG. 4A

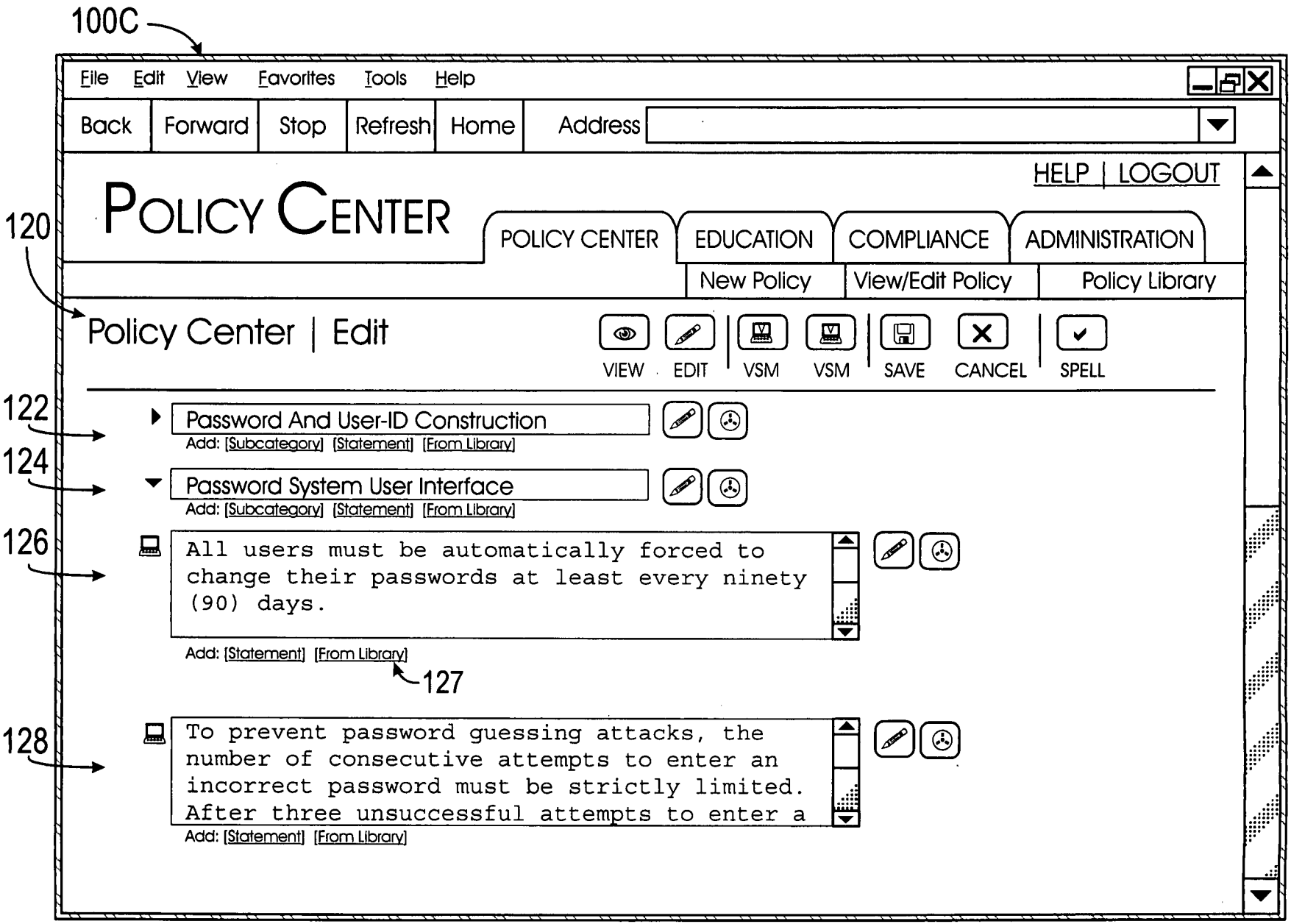

100C
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
HELP | LOGOUT
POLICY CENTER
120
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Policy View/Edit Policy Policy Library
Policy Center | Edit
VIEW EDIT VSM VSM SAVE CANCEL SPELL
122
Password And User-ID Construction
Add: [Subcategory] [Statement] [From Library]
124
Password System User Interface
Add: [Subcategory] [Statement] [From Library]
126
All users must be automatically forced to change their passwords at least every ninety (90) days.
Add: [Statement] [From Library]
127
128
To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a
Add: [Statement] [From Library]

FIG. 4B

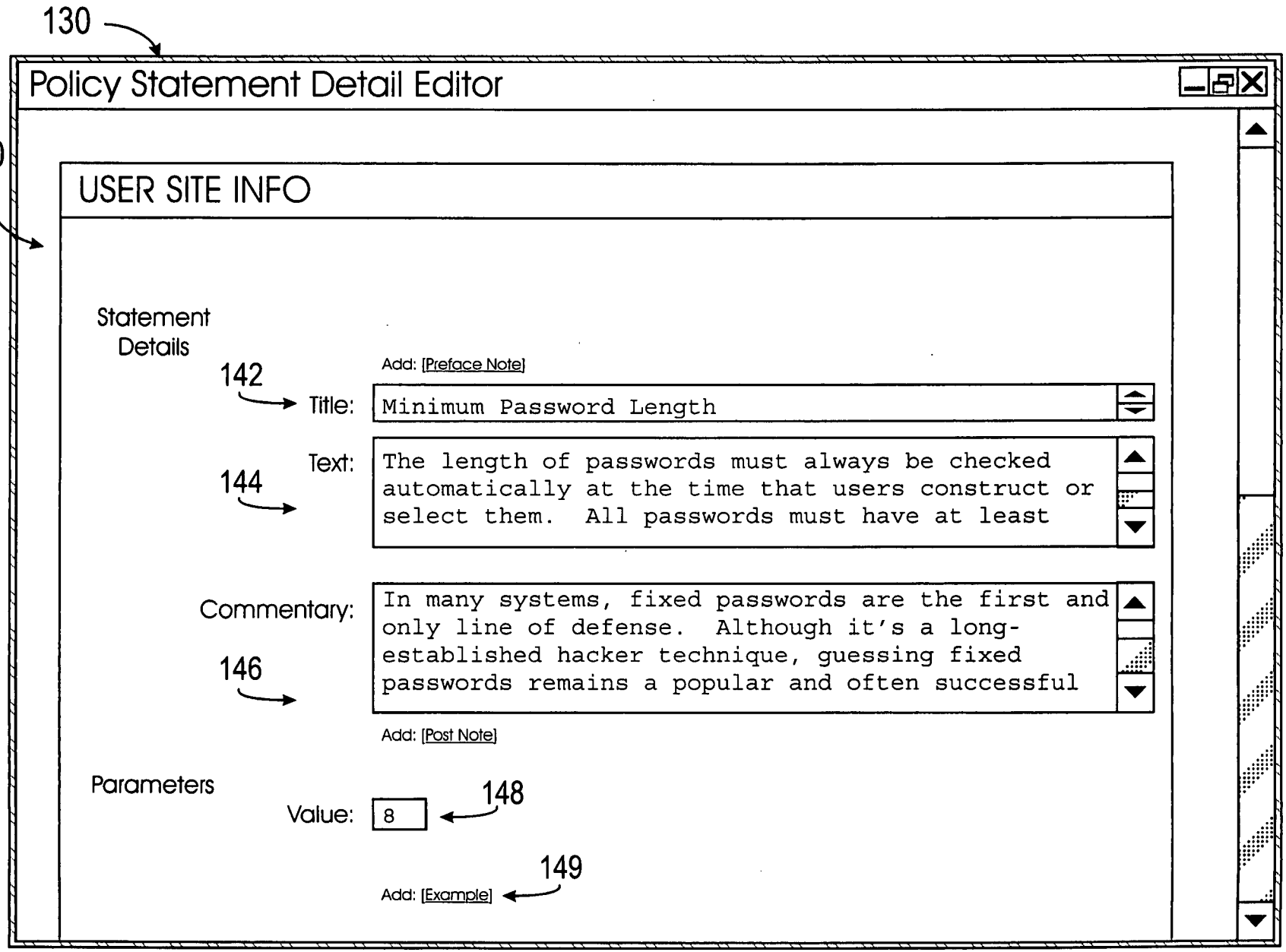

130
Policy Statement Detail Editor
140
USER SITE INFO
Statement Details
142
Add: [Preface Note]
Title:
Minimum Password Length
Text:
144
The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least
Commentary:
146
In many systems, fixed passwords are the first and only line of defense. Although it's a long-established hacker technique, guessing fixed passwords remains a popular and often successful
Add: [Post Note]
Parameters
Value:
8
148
149
Add: [Example]

FIG. 5A

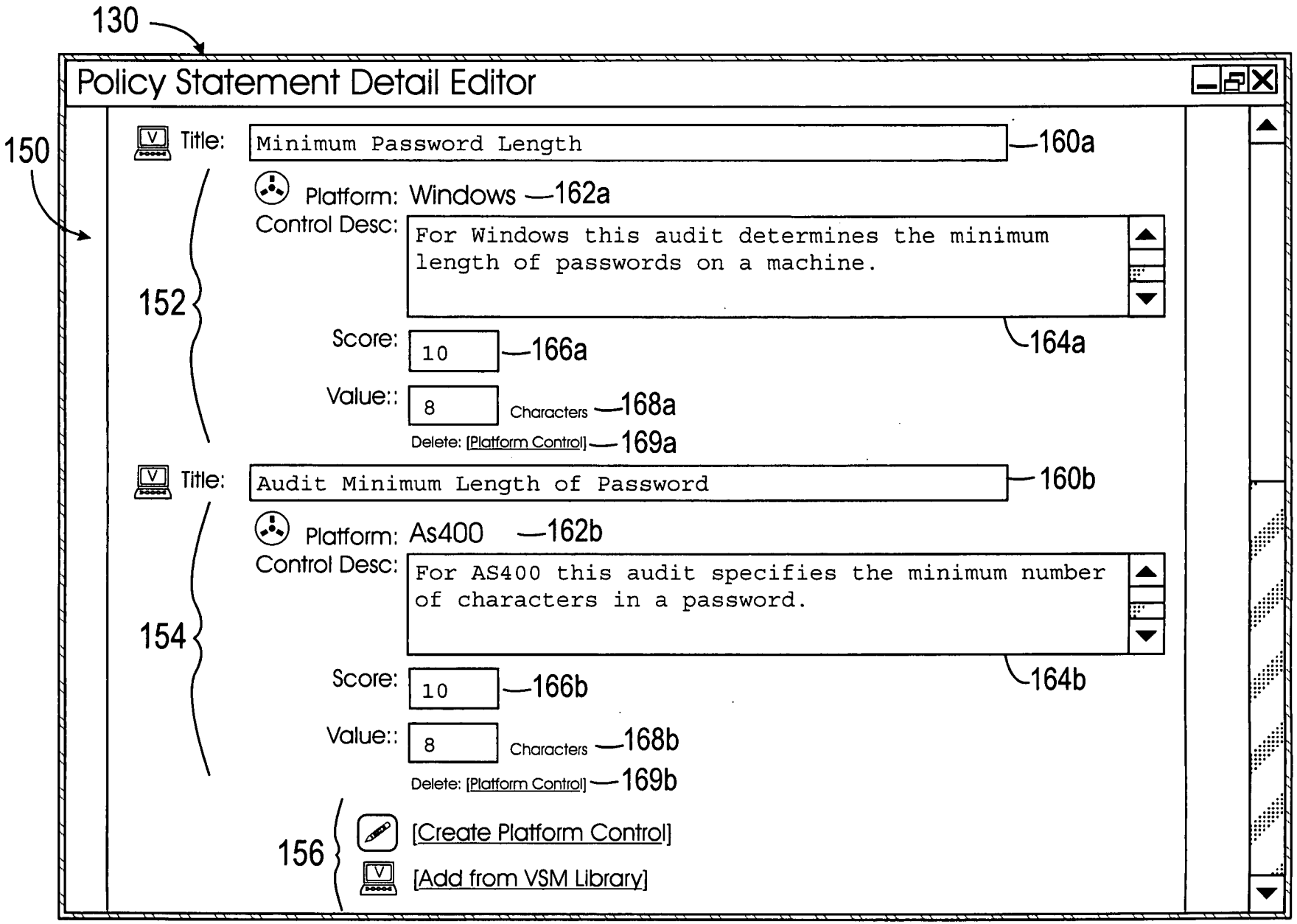

130
Policy Statement Detail Editor
150
Title:
Minimum Password Length
160a
Platform: Windows
162a
Control Desc:
For Windows this audit determines the minimum length of passwords on a machine.
152
164a
Score:
10
166a
Value::
8
Characters
168a
Delete: [Platform Control]
169a
Title:
Audit Minimum Length of Password
160b
Platform: As400
162b
Control Desc:
For AS400 this audit specifies the minimum number of characters in a password.
154
164b
Score:
10
166b
Value::
8
Characters
168b
Delete: [Platform Control]
169b
156
[Create Platform Control]
[Add from VSM Library]

FIG. 5B

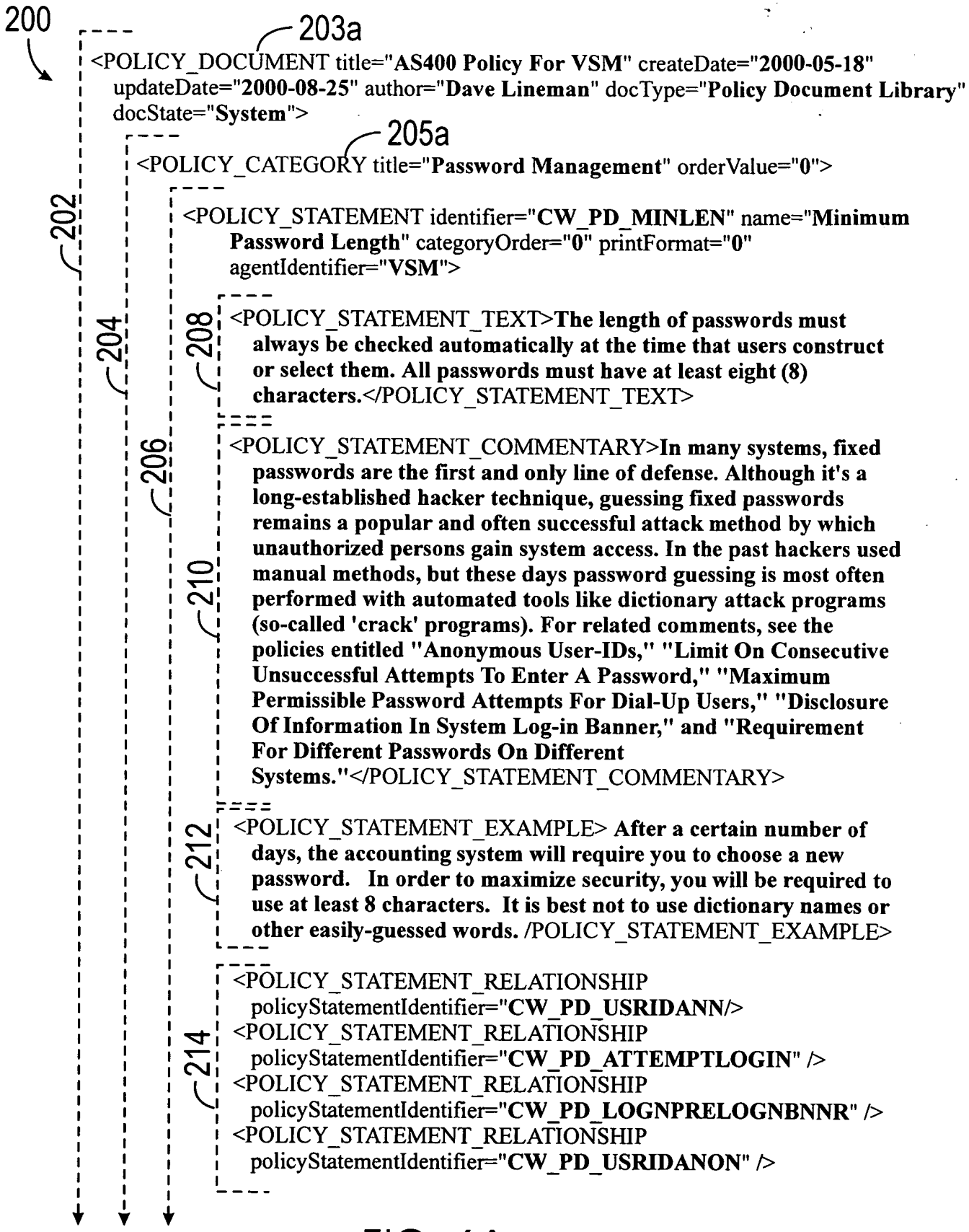

200
203a
<POLICY_DOCUMENT title="AS400 Policy For VSM" createDate="2000-05-18" updateDate="2000-08-25" author="Dave Lineman" docType="Policy Document Library" docState="System">
205a
<POLICY_CATEGORY title="Password Management" orderValue="0">
202
<POLICY_STATEMENT identifier="CW_PD_MINLEN" name="Minimum Password Length" categoryOrder="0" printFormat="0" agentIdentifier="VSM">
204
208
<POLICY_STATEMENT_TEXT>The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least eight (8) characters.</POLICY_STATEMENT_TEXT>
206
<POLICY_STATEMENT_COMMENTARY>In many systems, fixed passwords are the first and only line of defense. Although it's a long-established hacker technique, guessing fixed passwords remains a popular and often successful attack method by which unauthorized persons gain system access. In the past hackers used manual methods, but these days password guessing is most often performed with automated tools like dictionary attack programs (so-called 'crack' programs). For related comments, see the policies entitled "Anonymous User-IDs," "Limit On Consecutive Unsuccessful Attempts To Enter A Password," "Maximum Permissible Password Attempts For Dial-Up Users," "Disclosure Of Information In System Log-in Banner," and "Requirement For Different Passwords On Different Systems."</POLICY_STATEMENT_COMMENTARY>
210
<POLICY_STATEMENT_EXAMPLE> After a certain number of days, the accounting system will require you to choose a new password. In order to maximize security, you will be required to use at least 8 characters. It is best not to use dictionary names or other easily-guessed words. /POLICY_STATEMENT_EXAMPLE>
212
<POLICY_STATEMENT_RELATIONSHIP policyStatementIdentifier="CW_PD_USRIDANN/>
<POLICY_STATEMENT_RELATIONSHIP policyStatementIdentifier="CW_PD_ATTEMPTLOGIN" />
<POLICY_STATEMENT_RELATIONSHIP policyStatementIdentifier="CW_PD_LOGNPRELOGNBNNR" />
<POLICY_STATEMENT_RELATIONSHIP policyStatementIdentifier="CW_PD_USRIDANON" />
214

FIG. 6A

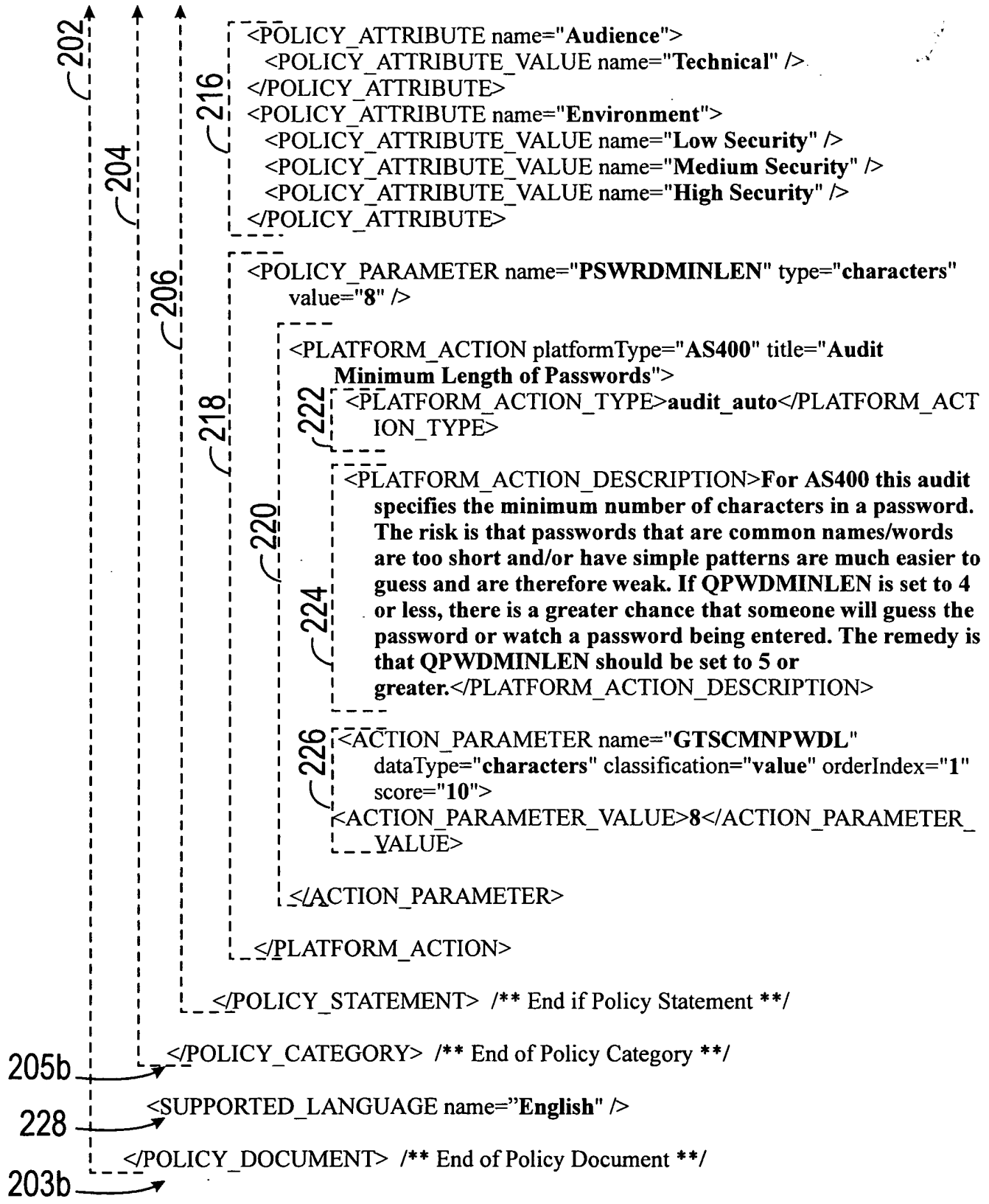

202
204
206
216
218
220
222
224
226
205b
228
203b
<POLICY_ATTRIBUTE name="Audience">
<POLICY_ATTRIBUTE_VALUE name="Technical" />
</POLICY_ATTRIBUTE>
<POLICY_ATTRIBUTE name="Environment">
<POLICY_ATTRIBUTE_VALUE name="Low Security" />
<POLICY_ATTRIBUTE_VALUE name="Medium Security" />
<POLICY_ATTRIBUTE_VALUE name="High Security" />
</POLICY_ATTRIBUTE>
<POLICY_PARAMETER name="PSWRDMINLEN" type="characters" value="8" />
<PLATFORM_ACTION platformType="AS400" title="Audit Minimum Length of Passwords">
<PLATFORM_ACTION_TYPE>audit_auto</PLATFORM_ACTION_TYPE>
<PLATFORM_ACTION_DESCRIPTION>For AS400 this audit specifies the minimum number of characters in a password. The risk is that passwords that are common names/words are too short and/or have simple patterns are much easier to guess and are therefore weak. If QPWDMINLEN is set to 4 or less, there is a greater chance that someone will guess the password or watch a password being entered. The remedy is that QPWDMINLEN should be set to 5 or greater.</PLATFORM_ACTION_DESCRIPTION>
<ACTION_PARAMETER name="GTSCMNPWDL" dataType="characters" classification="value" orderIndex="1" score="10">
<ACTION_PARAMETER_VALUE>8</ACTION_PARAMETER_VALUE>
</ACTION_PARAMETER>
</PLATFORM_ACTION>
</POLICY_STATEMENT> /** End if Policy Statement **/
</POLICY_CATEGORY> /** End of Policy Category **/
<SUPPORTED_LANGUAGE name="English" />
</POLICY_DOCUMENT> /** End of Policy Document **/

FIG. 6B

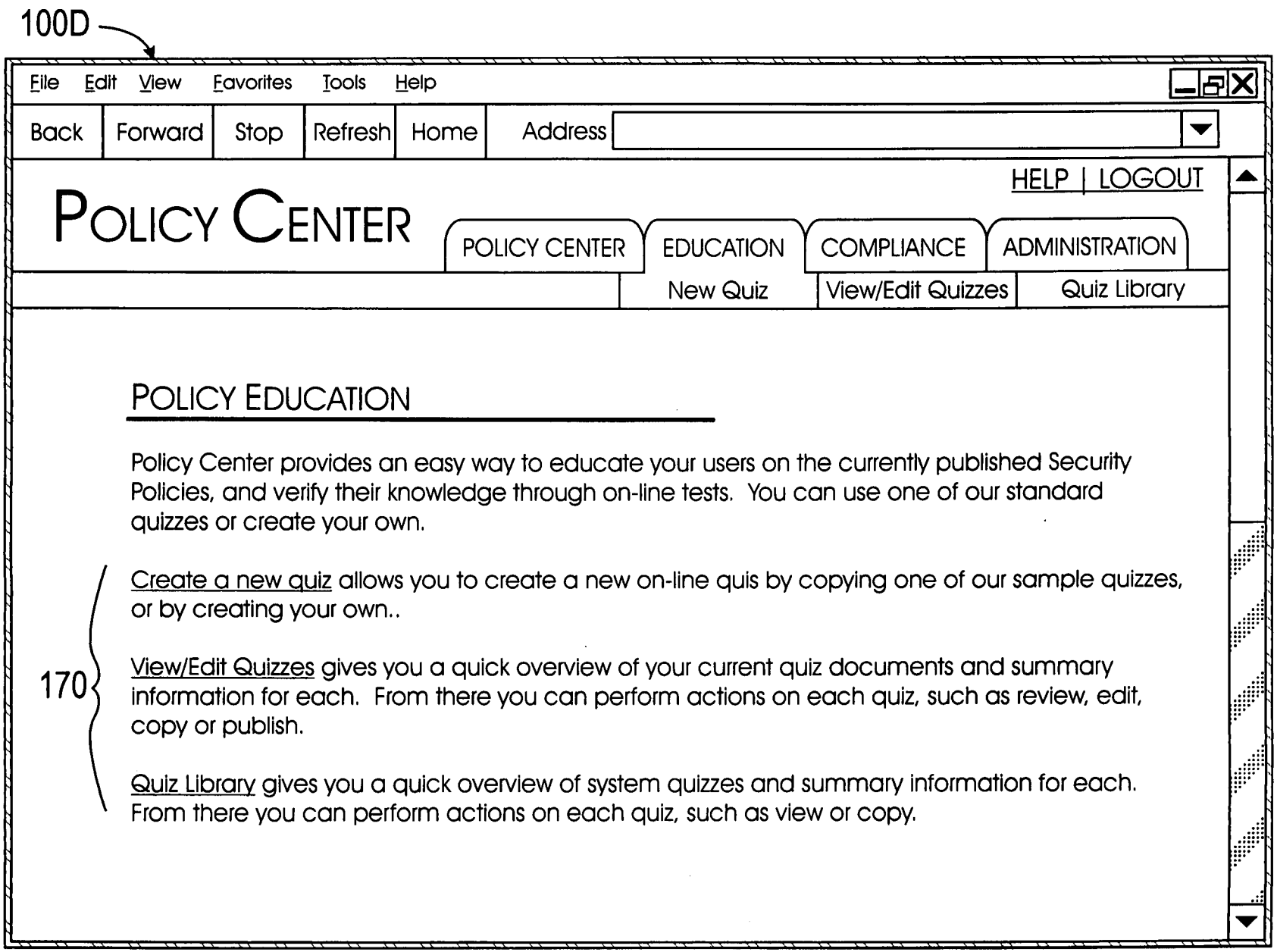

100D
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Quiz View/Edit Quizzes Quiz Library
POLICY EDUCATION
Policy Center provides an easy way to educate your users on the currently published Security Policies, and verify their knowledge through on-line tests. You can use one of our standard quizzes or create your own.
Create a new quiz allows you to create a new on-line quis by copying one of our sample quizzes, or by creating your own..
View/Edit Quizzes gives you a quick overview of your current quiz documents and summary information for each. From there you can perform actions on each quiz, such as review, edit, copy or publish.
Quiz Library gives you a quick overview of system quizzes and summary information for each. From there you can perform actions on each quiz, such as view or copy.
170

FIG. 7A

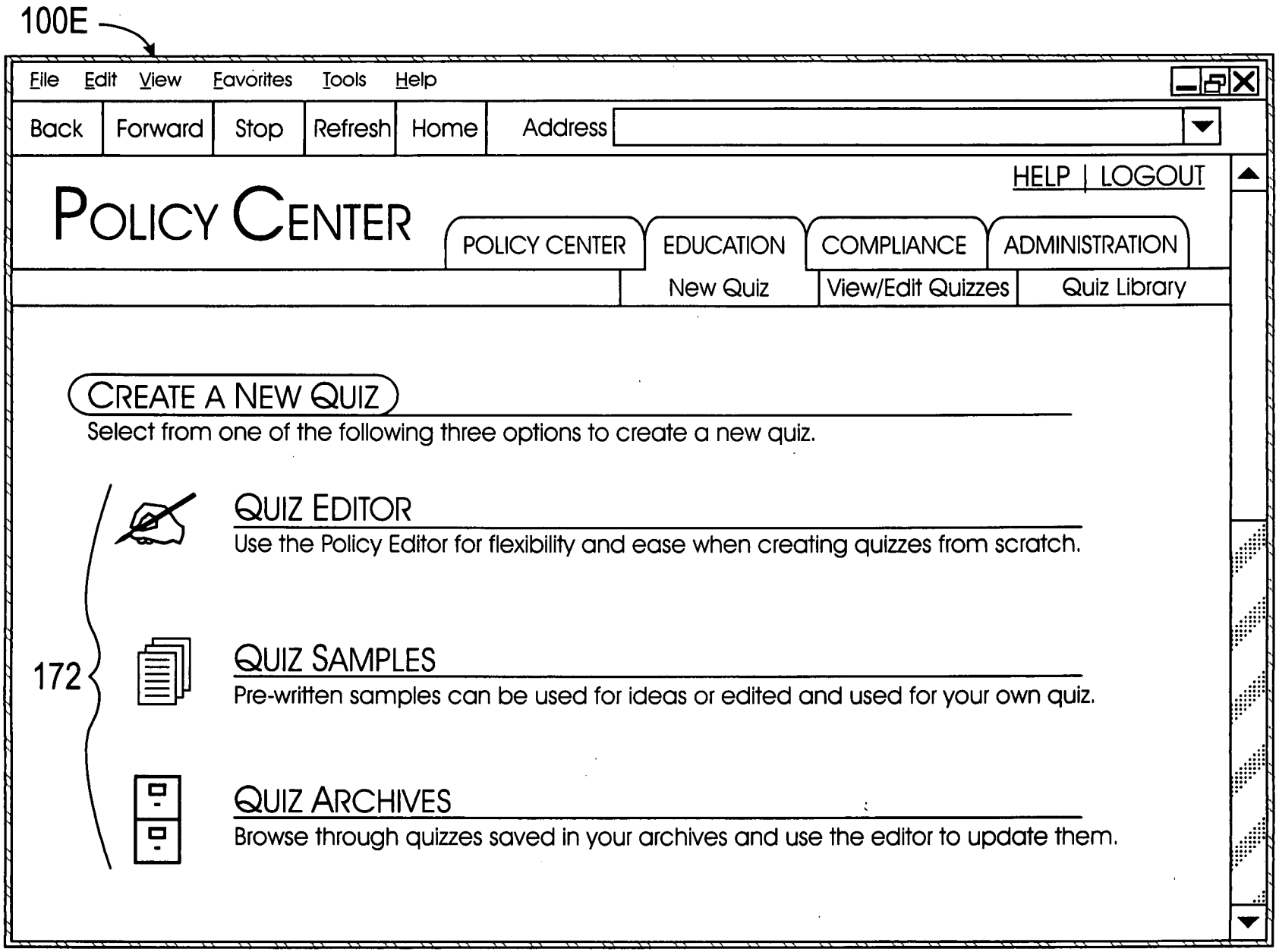

100E
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Quiz View/Edit Quizzes Quiz Library
CREATE A NEW QUIZ
Select from one of the following three options to create a new quiz.
QUIZ EDITOR
Use the Policy Editor for flexibility and ease when creating quizzes from scratch.
172
QUIZ SAMPLES
Pre-written samples can be used for ideas or edited and used for your own quiz.
QUIZ ARCHIVES
Browse through quizzes saved in your archives and use the editor to update them.

FIG. 7B

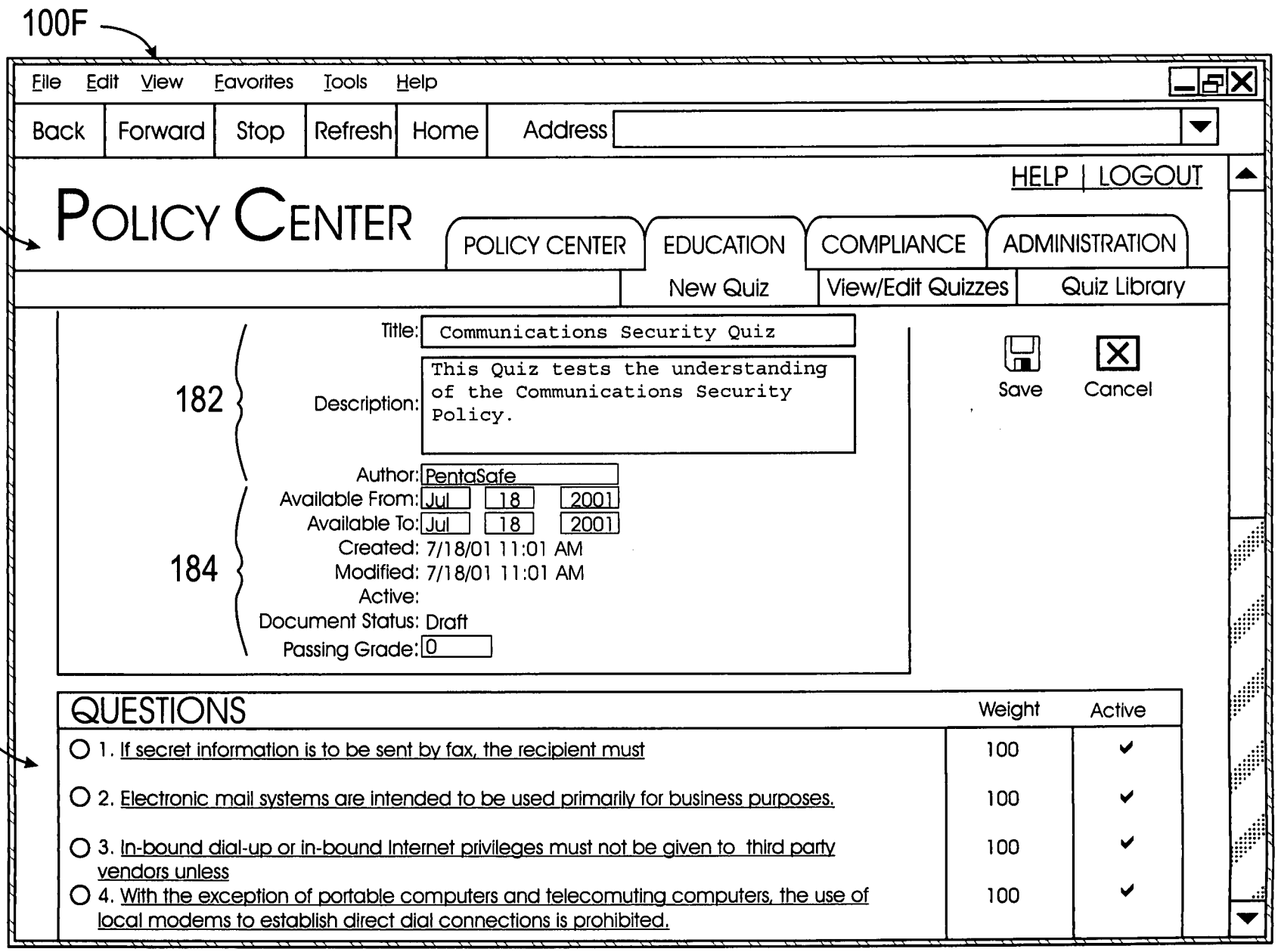

100F
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
180
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Quiz View/Edit Quizzes Quiz Library
Title: Communications Security Quiz
182
Description: This Quiz tests the understanding of the Communications Security Policy.
Save Cancel
Author: PentaSafe
Available From: Jul 18 2001
Available To: Jul 18 2001
184
Created: 7/18/01 11:01 AM
Modified: 7/18/01 11:01 AM
Active:
Document Status: Draft
Passing Grade: 0
186
QUESTIONS Weight Active
1. If secret information is to be sent by fax, the recipient must 100
2. Electronic mail systems are intended to be used primarily for business purposes. 100
3. In-bound dial-up or in-bound Internet privileges must not be given to third party vendors unless 100
4. With the exception of portable computers and telecomuting computers, the use of local modems to establish direct dial connections is prohibited. 100

FIG. 7C

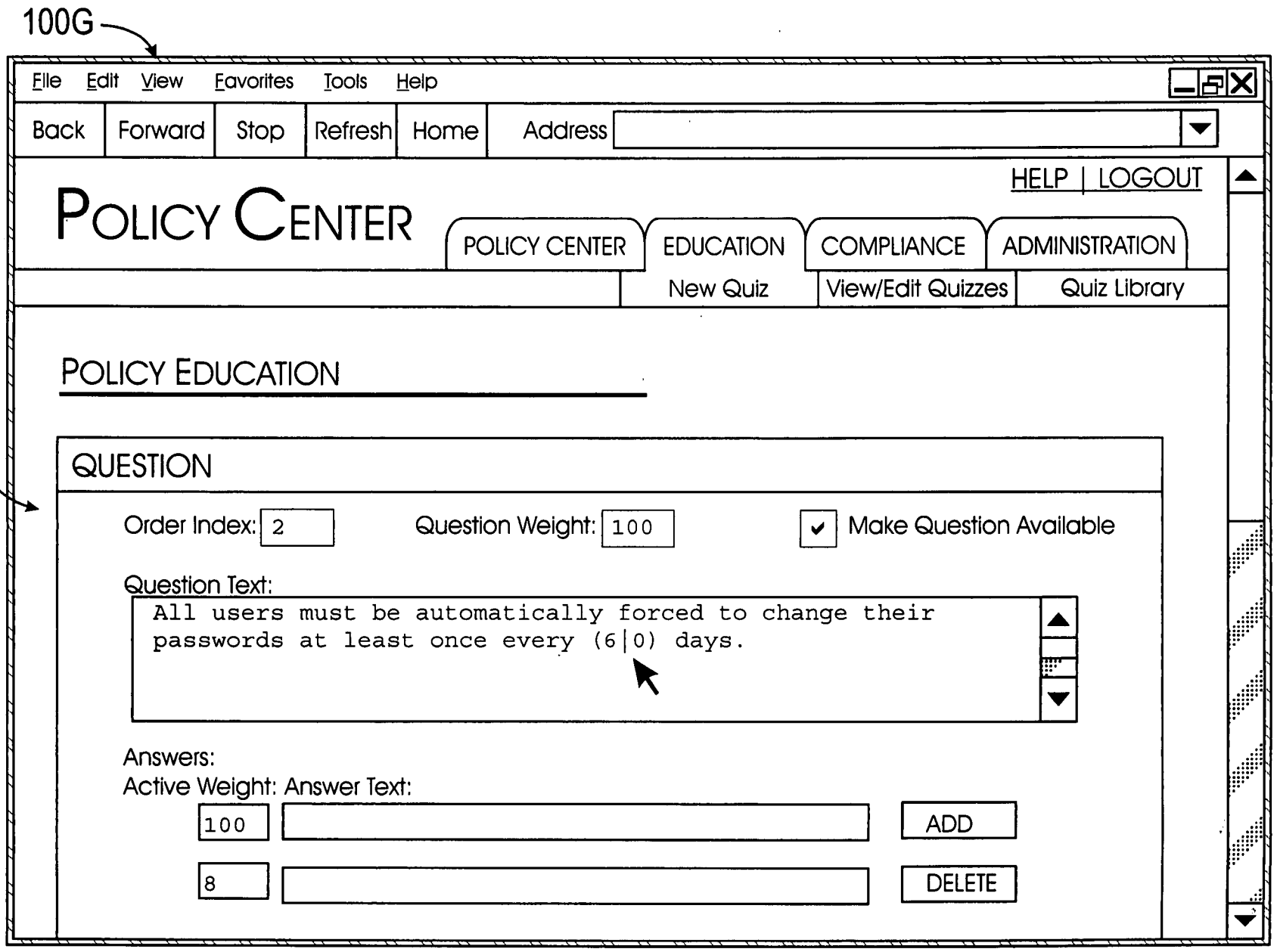

100G
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Quiz View/Edit Quizzes Quiz Library
POLICY EDUCATION
186'
QUESTION
Order Index: 2
Question Weight: 100
Make Question Available
Question Text:
All users must be automatically forced to change their passwords at least once every (6|0) days.
Answers:
Active Weight: Answer Text:
100
ADD
8
DELETE

FIG. 7D

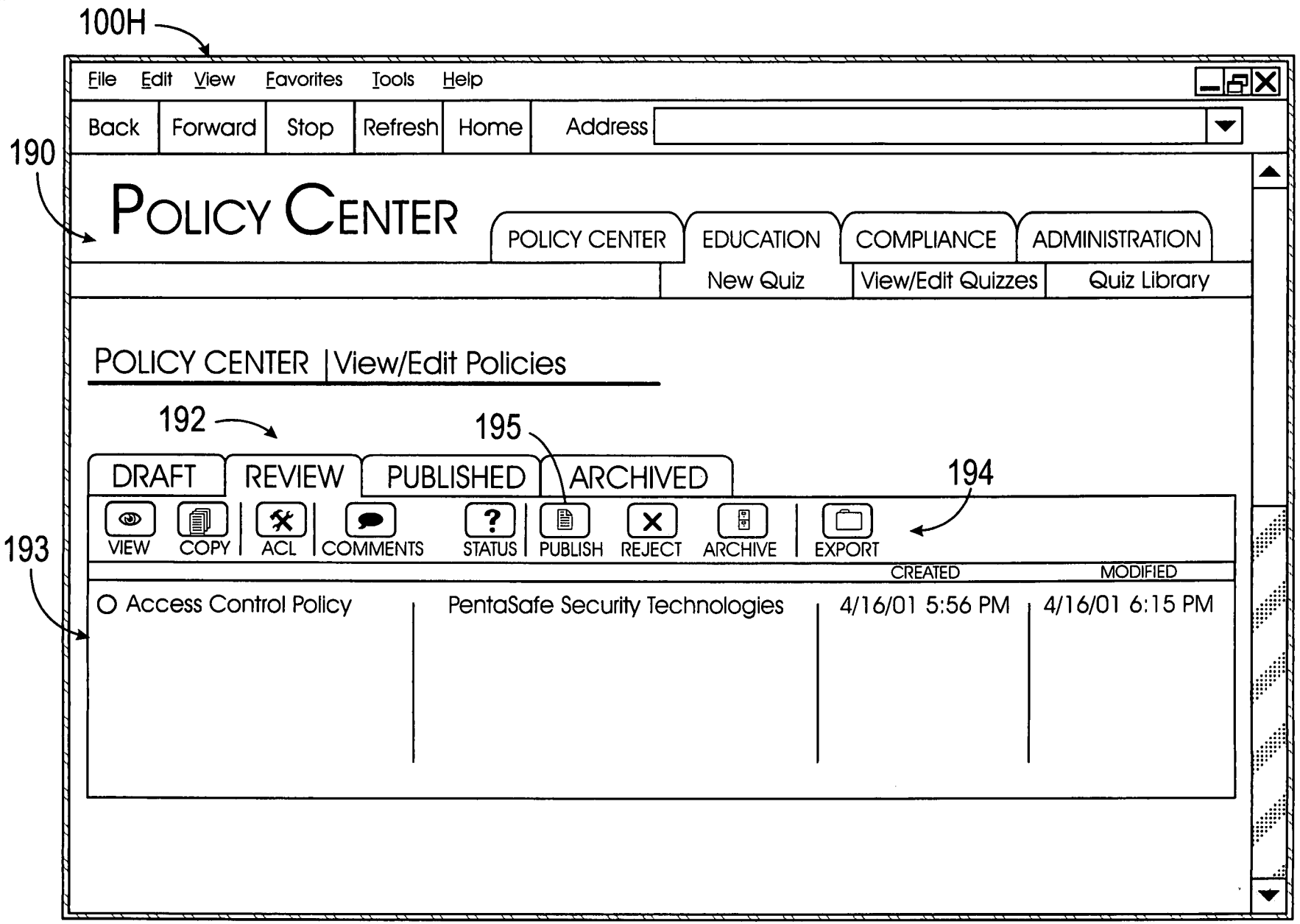
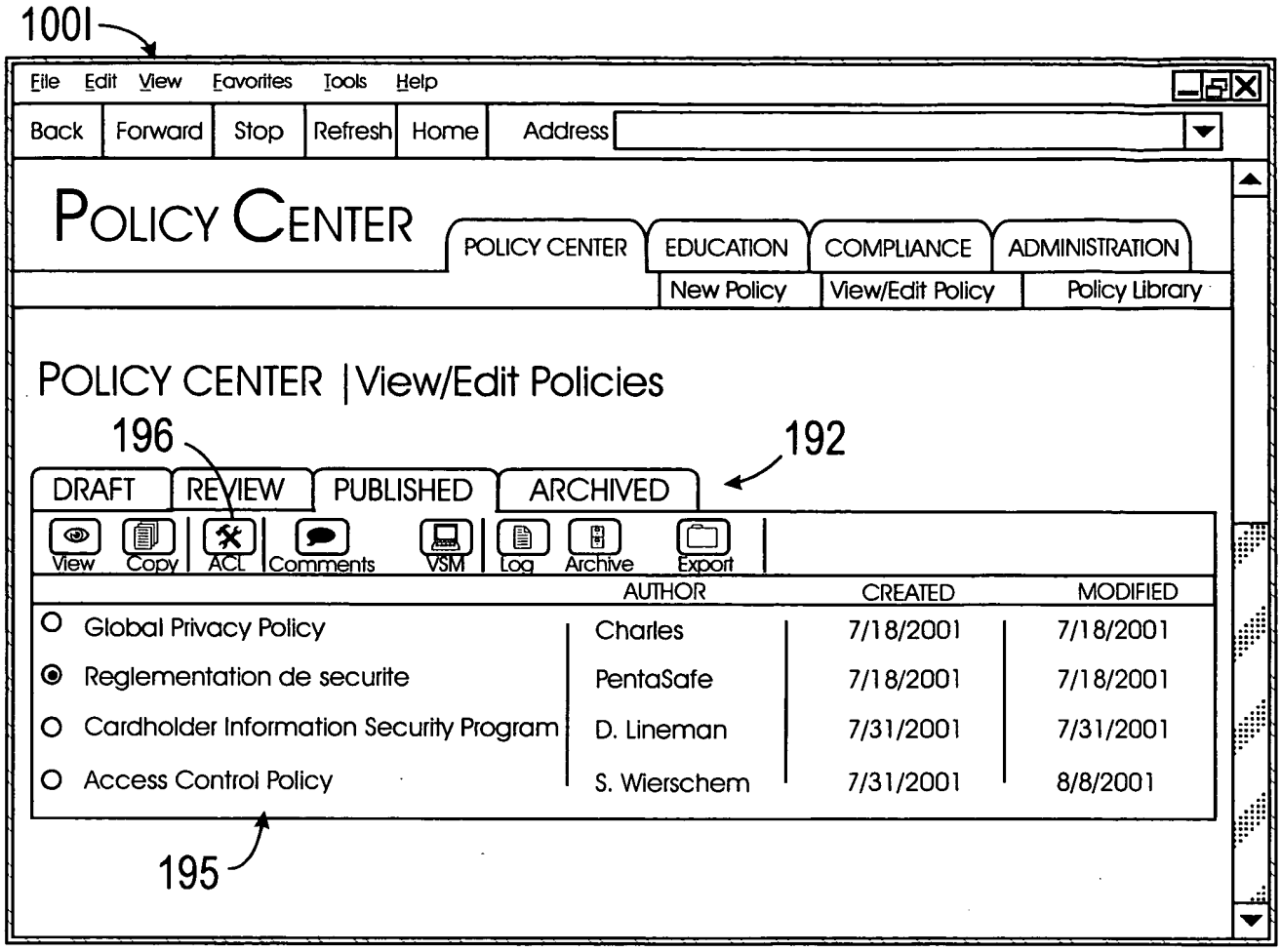

100H
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
190
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Quiz View/Edit Quizzes Quiz Library
POLICY CENTER | View/Edit Policies
192
195
DRAFT REVIEW PUBLISHED ARCHIVED
194
VIEW COPY ACL COMMENTS STATUS PUBLISH REJECT ARCHIVE EXPORT
193
CREATED MODIFIED
O Access Control Policy
PentaSafe Security Technologies
4/16/01 5:56 PM
4/16/01 6:15 PM

FIG. 8


1001
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
New Policy View/Edit Policy Policy Library
POLICY CENTER | View/Edit Policies
196
192
DRAFT REVIEW PUBLISHED ARCHIVED
View Copy ACL Comments VSM Log Archive Export
AUTHOR CREATED MODIFIED
Global Privacy Policy Charles 7/18/2001 7/18/2001
Reglementation de securite PentaSafe 7/18/2001 7/18/2001
Cardholder Information Security Program D. Lineman 7/31/2001 7/31/2001
Access Control Policy S. Wierschem 7/31/2001 8/8/2001
195

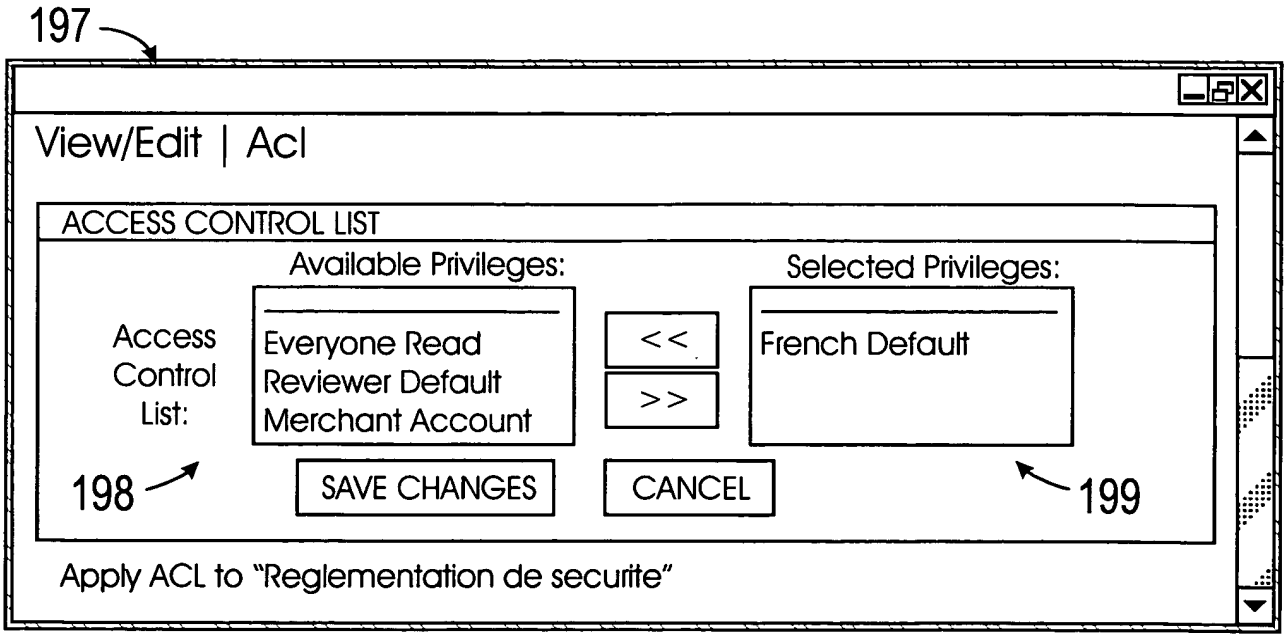

197
View/Edit | Acl
ACCESS CONTROL LIST
Available Privileges:
Selected Privileges:
Access Control List:
Everyone Read
Reviewer Default
Merchant Account
<<
>>
French Default
198
SAVE CHANGES
CANCEL
199
Apply ACL to "Reglementation de securite"

FIG. 9

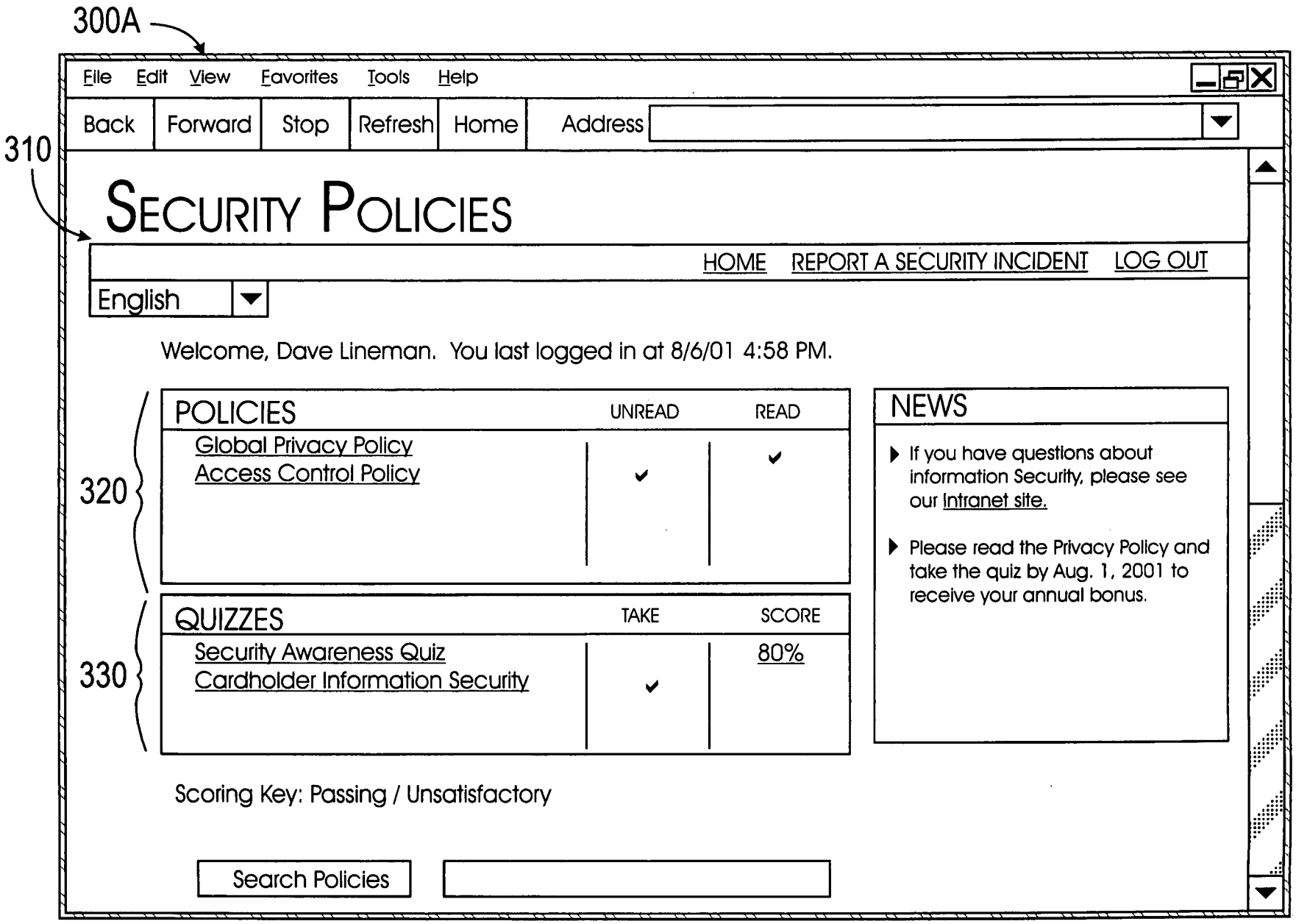
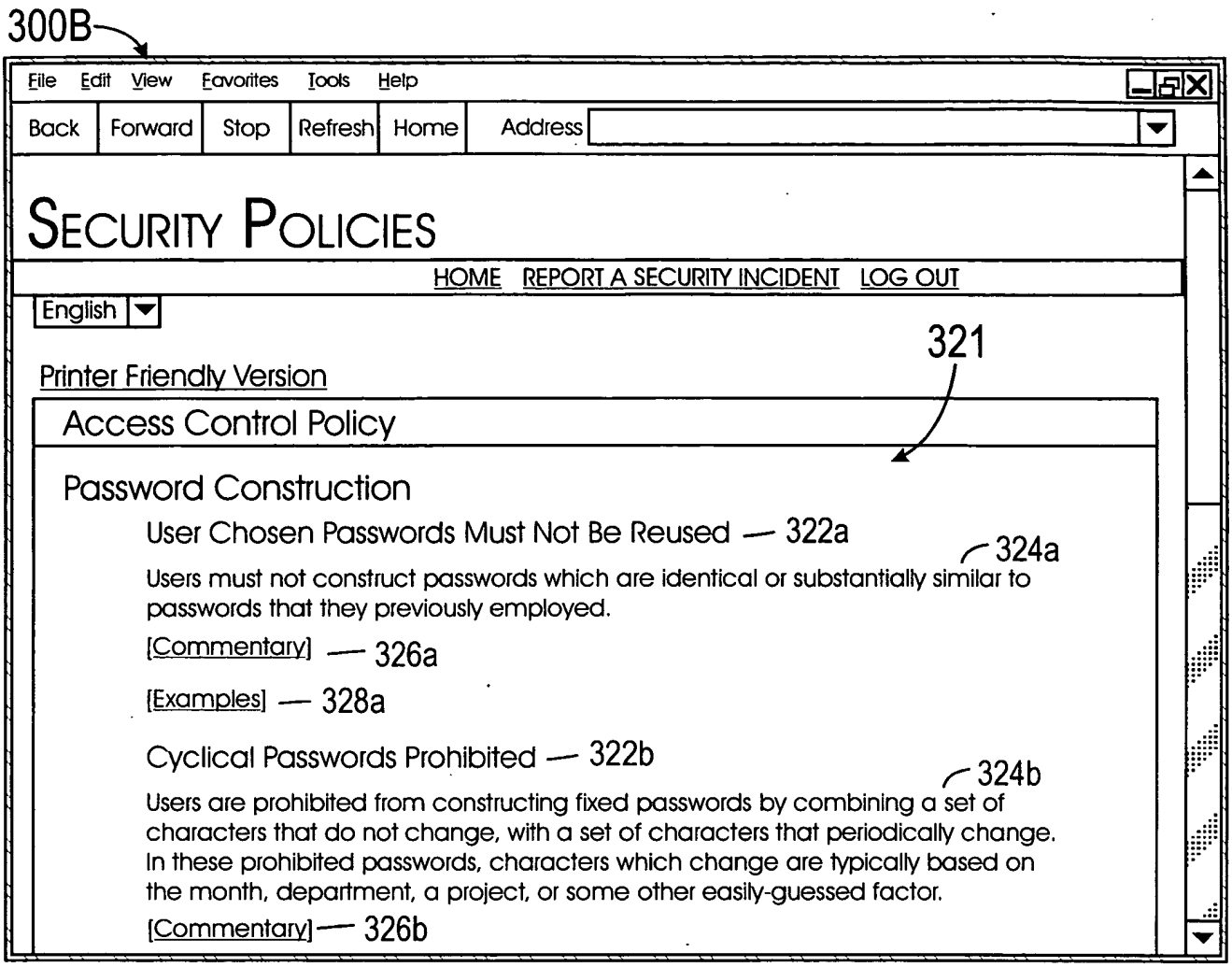

300A
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
310
SECURITY POLICIES
HOME REPORT A SECURITY INCIDENT LOG OUT
English
Welcome, Dave Lineman. You last logged in at 8/6/01 4:58 PM.
320
POLICIES UNREAD READ
Global Privacy Policy
Access Control Policy
330
QUIZZES TAKE SCORE
Security Awareness Quiz 80%
Cardholder Information Security
NEWS
If you have questions about information Security, please see our Intranet site.
Please read the Privacy Policy and take the quiz by Aug. 1, 2001 to receive your annual bonus.
Scoring Key: Passing / Unsatisfactory
Search Policies

FIG. 10A


300B
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
SECURITY POLICIES
HOME REPORT A SECURITY INCIDENT LOG OUT
English
321
Printer Friendly Version
Access Control Policy
Password Construction
User Chosen Passwords Must Not Be Reused — 322a
324a
Users must not construct passwords which are identical or substantially similar to passwords that they previously employed.
[Commentary] — 326a
[Examples] — 328a
Cyclical Passwords Prohibited — 322b
324b
Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that periodically change. In these prohibited passwords, characters which change are typically based on the month, department, a project, or some other easily-guessed factor.
[Commentary] — 326b

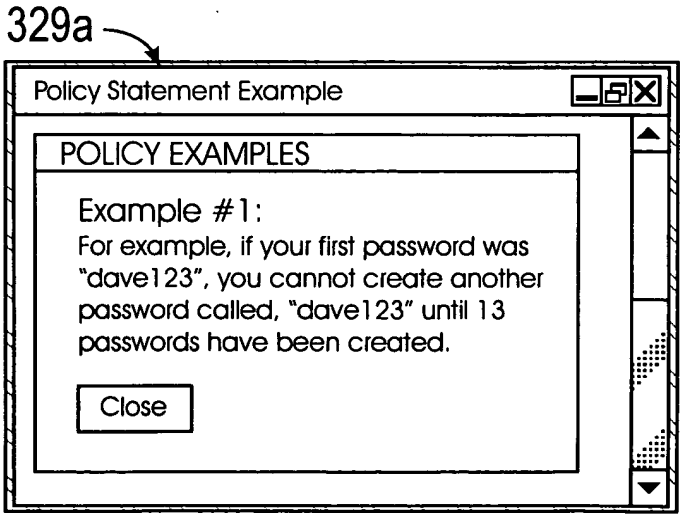

329a
Policy Statement Example
POLICY EXAMPLES
Example #1:
For example, if your first password was "dave123", you cannot create another password called, "dave123" until 13 passwords have been created.
Close

FIG. 10B

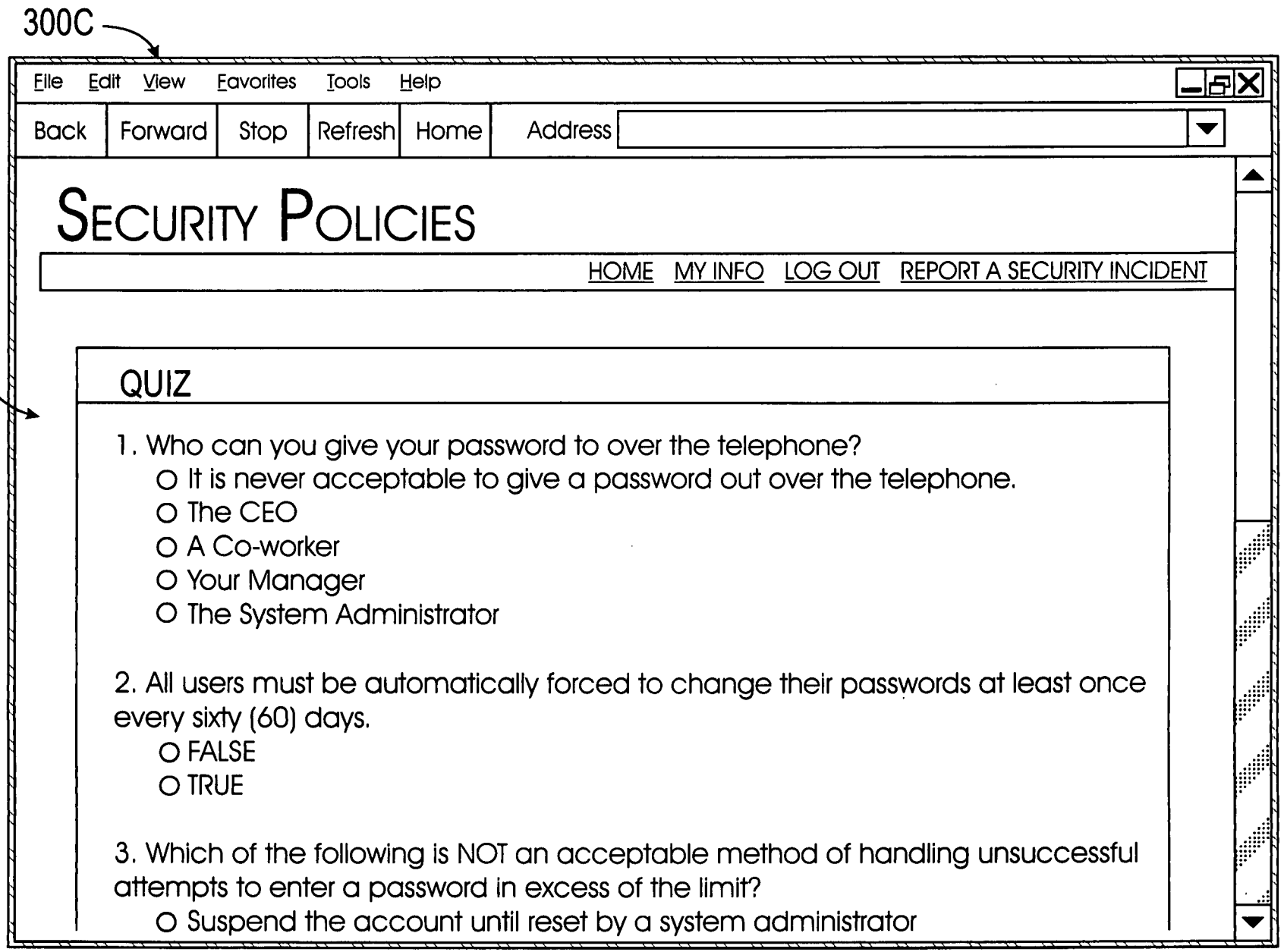

300C
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
SECURITY POLICIES
HOME MY INFO LOG OUT REPORT A SECURITY INCIDENT
331
QUIZ
1. Who can you give your password to over the telephone?
O It is never acceptable to give a password out over the telephone.
O The CEO
O A Co-worker
O Your Manager
O The System Administrator
2. All users must be automatically forced to change their passwords at least once every sixty (60) days.
O FALSE
O TRUE
3. Which of the following is NOT an acceptable method of handling unsuccessful attempts to enter a password in excess of the limit?
O Suspend the account until reset by a system administrator

FIG. 10C

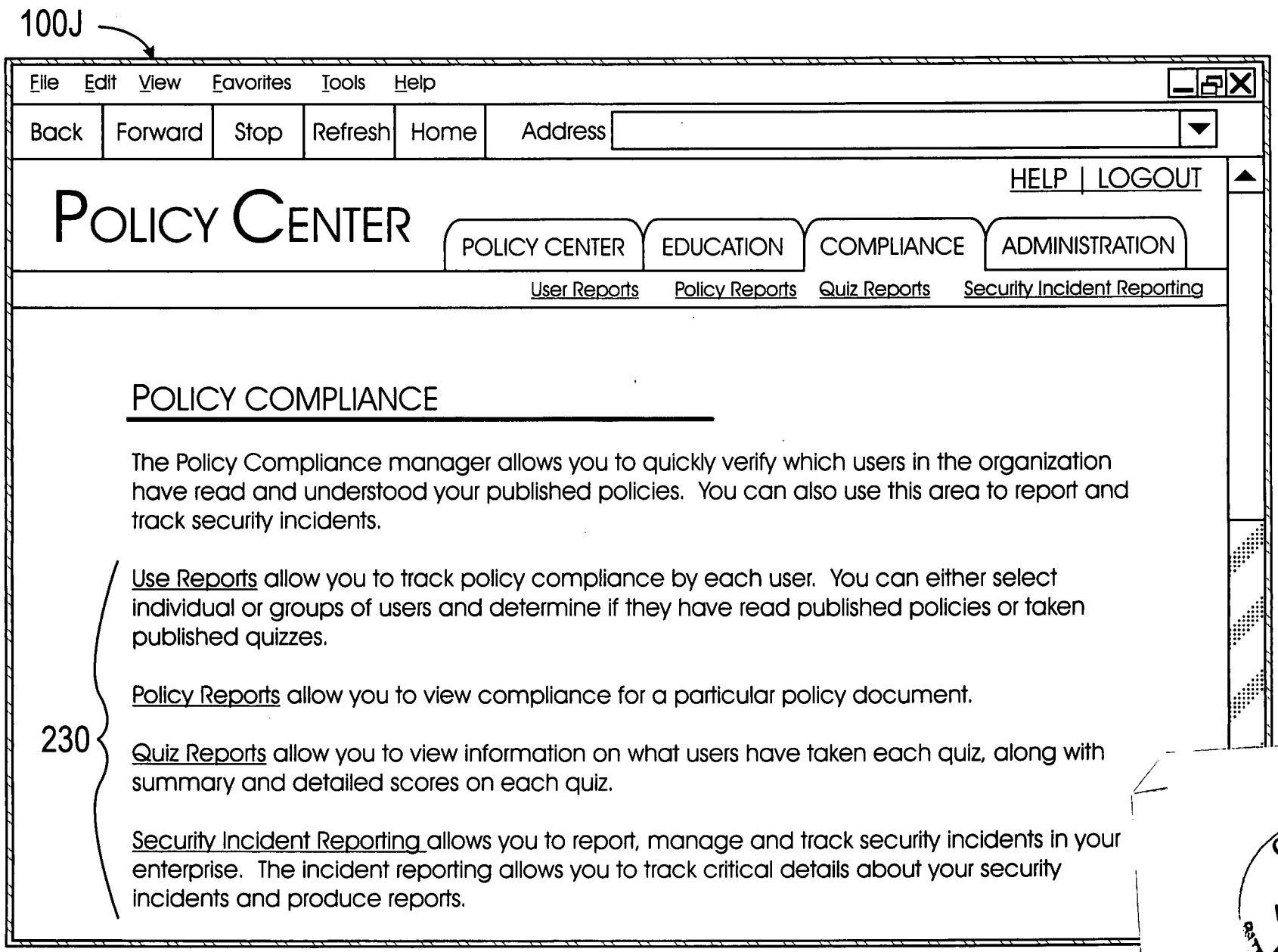



FIG. 11A

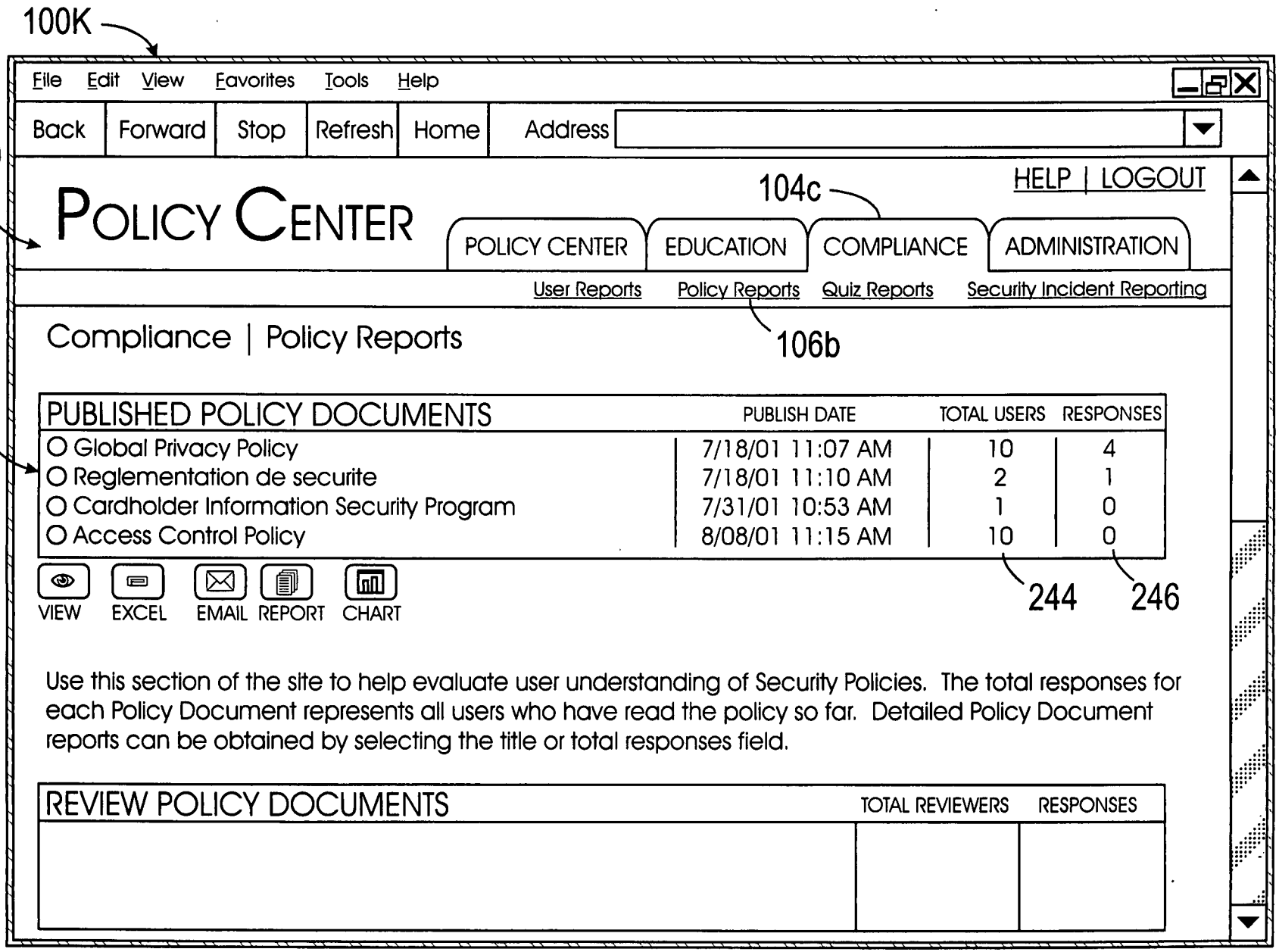

100K
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
240
POLICY CENTER
HELP | LOGOUT
104c
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
User Reports Policy Reports Quiz Reports Security Incident Reporting
Compliance | Policy Reports
106b
242
PUBLISHED POLICY DOCUMENTS
PUBLISH DATE
TOTAL USERS
RESPONSES
O Global Privacy Policy 7/18/01 11:07 AM 10 4
O Reglementation de securite 7/18/01 11:10 AM 2 1
O Cardholder Information Security Program 7/31/01 10:53 AM 1 0
O Access Control Policy 8/08/01 11:15 AM 10 0
VIEW EXCEL EMAIL REPORT CHART
244
246
Use this section of the site to help evaluate user understanding of Security Policies. The total responses for each Policy Document represents all users who have read the policy so far. Detailed Policy Document reports can be obtained by selecting the title or total responses field.
REVIEW POLICY DOCUMENTS
TOTAL REVIEWERS
RESPONSES

FIG. 11B

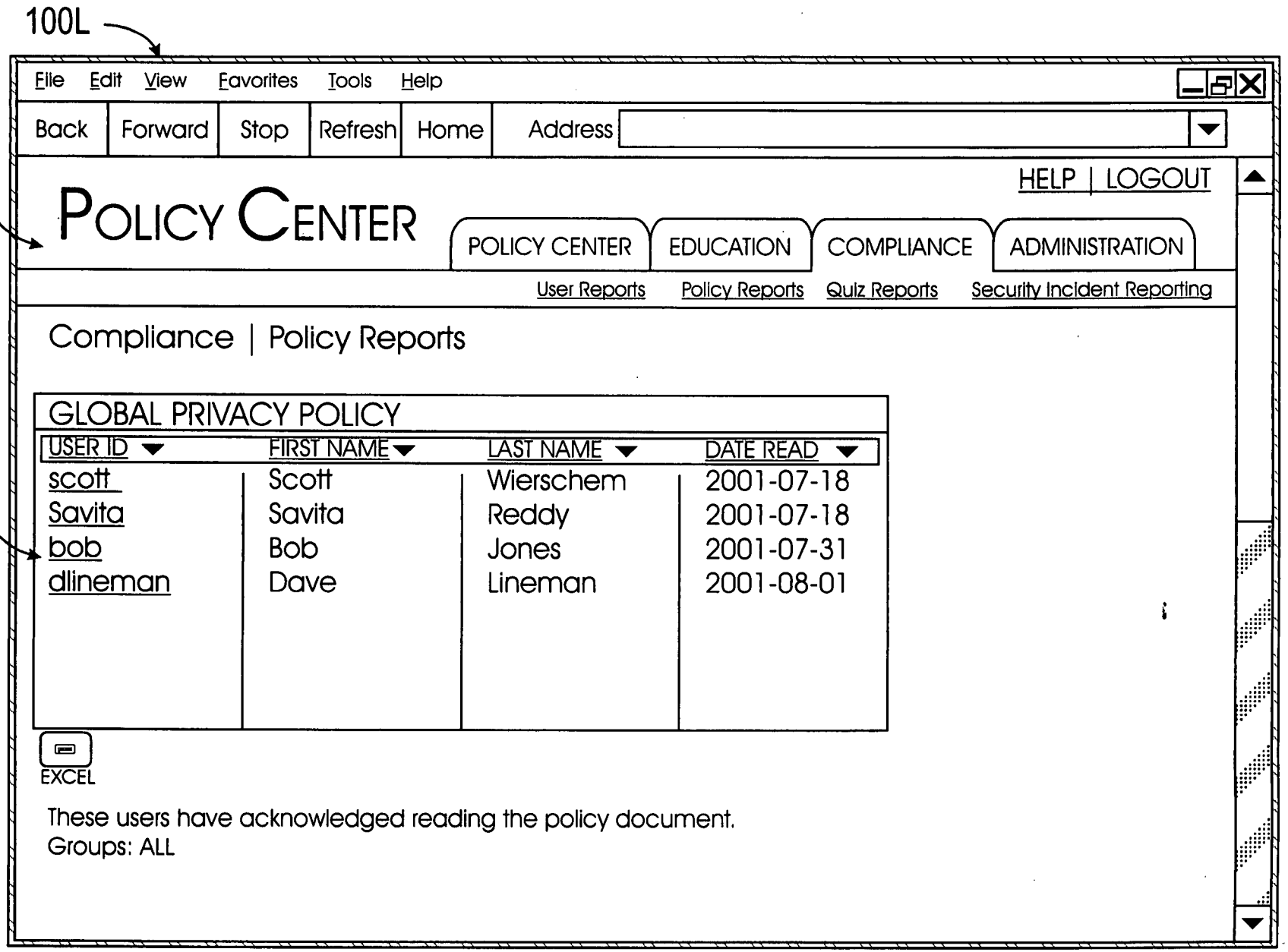

100L
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
250
POLICY CENTER
HELP | LOGOUT
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
User Reports Policy Reports Quiz Reports Security Incident Reporting
Compliance | Policy Reports
GLOBAL PRIVACY POLICY
252
USER ID FIRST NAME LAST NAME DATE READ
scott Scott Wierschem 2001-07-18
Savita Savita Reddy 2001-07-18
bob Bob Jones 2001-07-31
dlineman Dave Lineman 2001-08-01
EXCEL
These users have acknowledged reading the policy document.
Groups: ALL

FIG. 11C

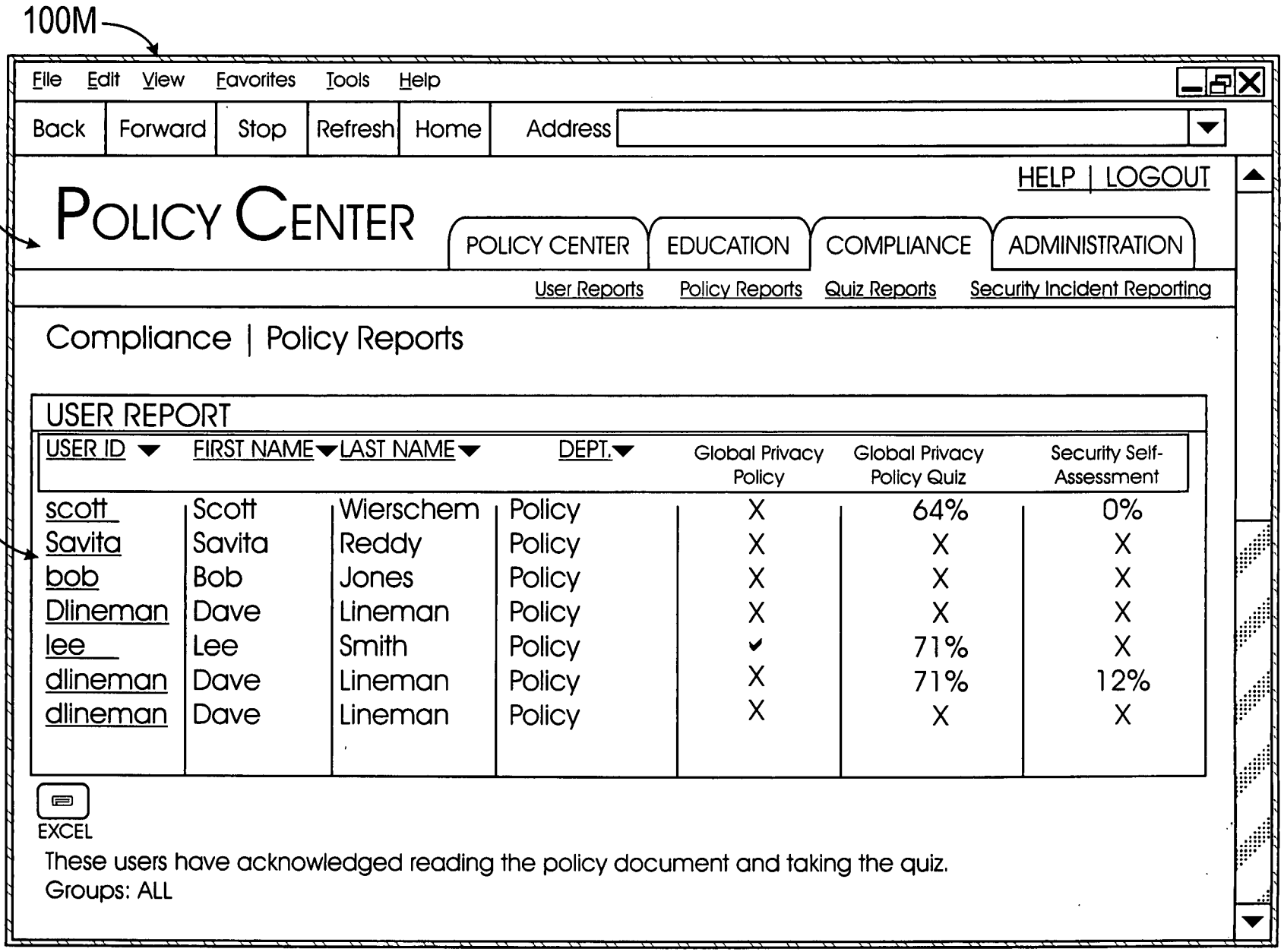

100M
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Address
260
HELP | LOGOUT
POLICY CENTER
POLICY CENTER EDUCATION COMPLIANCE ADMINISTRATION
User Reports Policy Reports Quiz Reports Security Incident Reporting
Compliance | Policy Reports
USER REPORT
262
USER ID FIRST NAME LAST NAME DEPT. Global Privacy Policy Global Privacy Policy Quiz Security Self-Assessment
scott Scott Wierschem Policy X 64% 0%
Savita Savita Reddy Policy X X X
bob Bob Jones Policy X X X
Dlineman Dave Lineman Policy X X X
lee Lee Smith Policy ✔ 71% X
dlineman Dave Lineman Policy X 71% 12%
dlineman Dave Lineman Policy X X X
EXCEL
These users have acknowledged reading the policy document and taking the quiz.
Groups: ALL

FIG. 11D

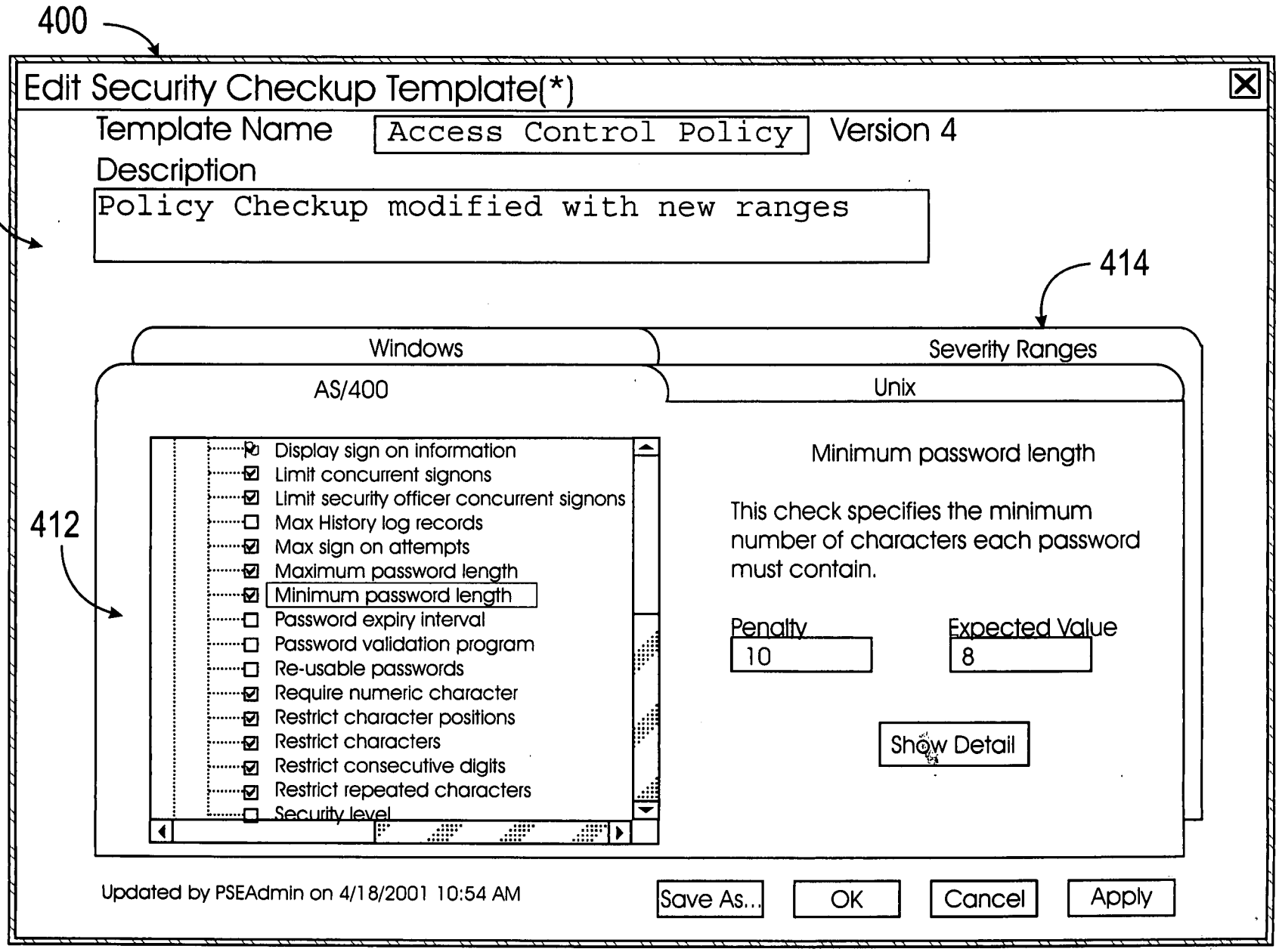

400
Edit Security Checkup Template(*)
Template Name
Access Control Policy
Version 4
410
Description
Policy Checkup modified with new ranges
414
Windows
Severity Ranges
AS/400
Unix
412
Display sign on information
Limit concurrent signons
Limit security officer concurrent signons
Max History log records
Max sign on attempts
Maximum password length
Minimum password length
Password expiry interval
Password validation program
Re-usable passwords
Require numeric character
Restrict character positions
Restrict characters
Restrict consecutive digits
Restrict repeated characters
Security level
Minimum password length
This check specifies the minimum number of characters each password must contain.
Penalty
10
Expected Value
8
Show Detail
Updated by PSEAdmin on 4/18/2001 10:54 AM
Save As...
OK
Cancel
Apply

FIG. 12

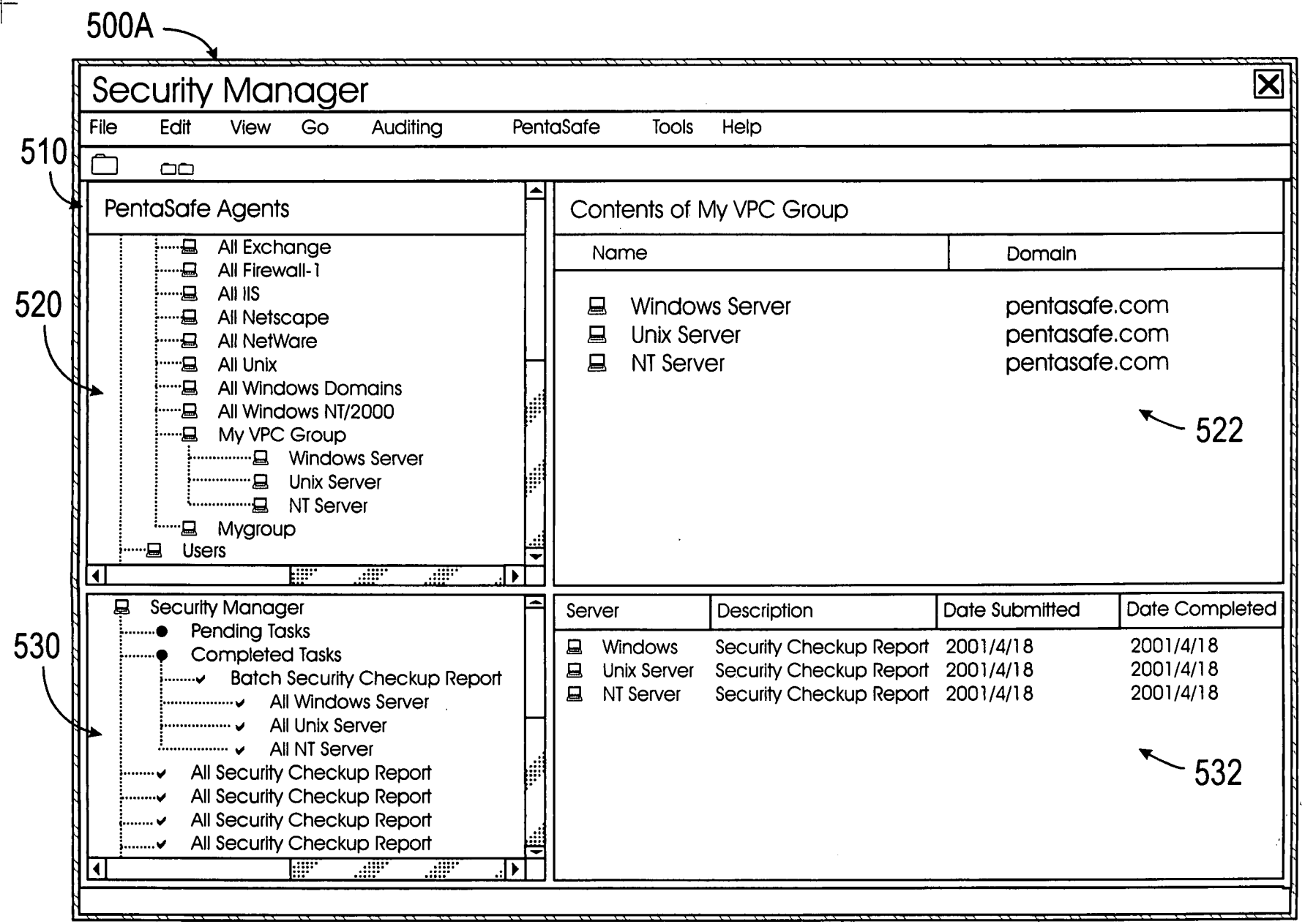



FIG. 13A

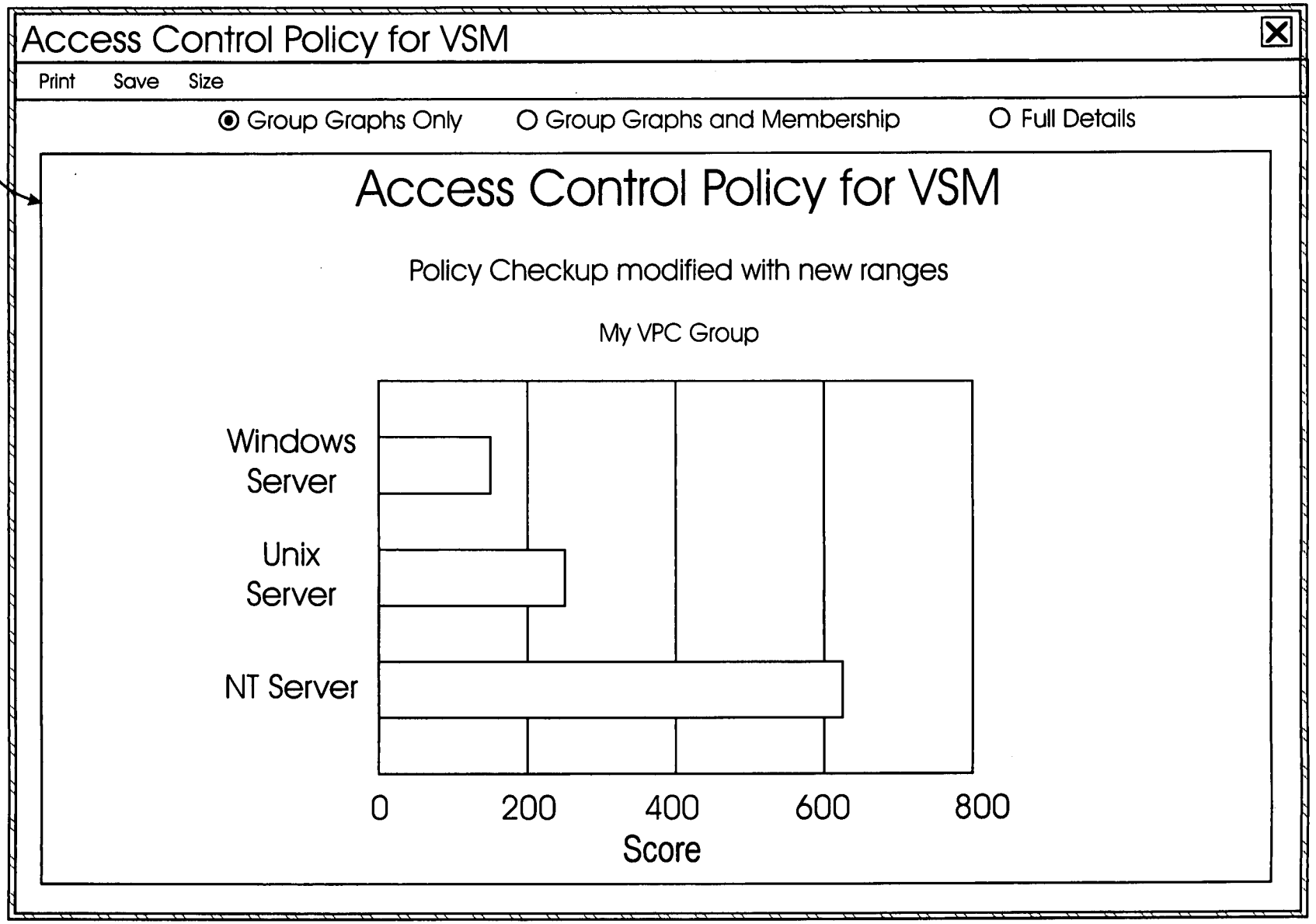

Access Control Policy for VSM
Print
Save
Size
540
Group Graphs Only
Group Graphs and Membership
Full Details
Access Control Policy for VSM
Policy Checkup modified with new ranges
My VPC Group
Windows Server
Unix Server
NT Server
0
200
400
600
800
Score

FIG. 13B

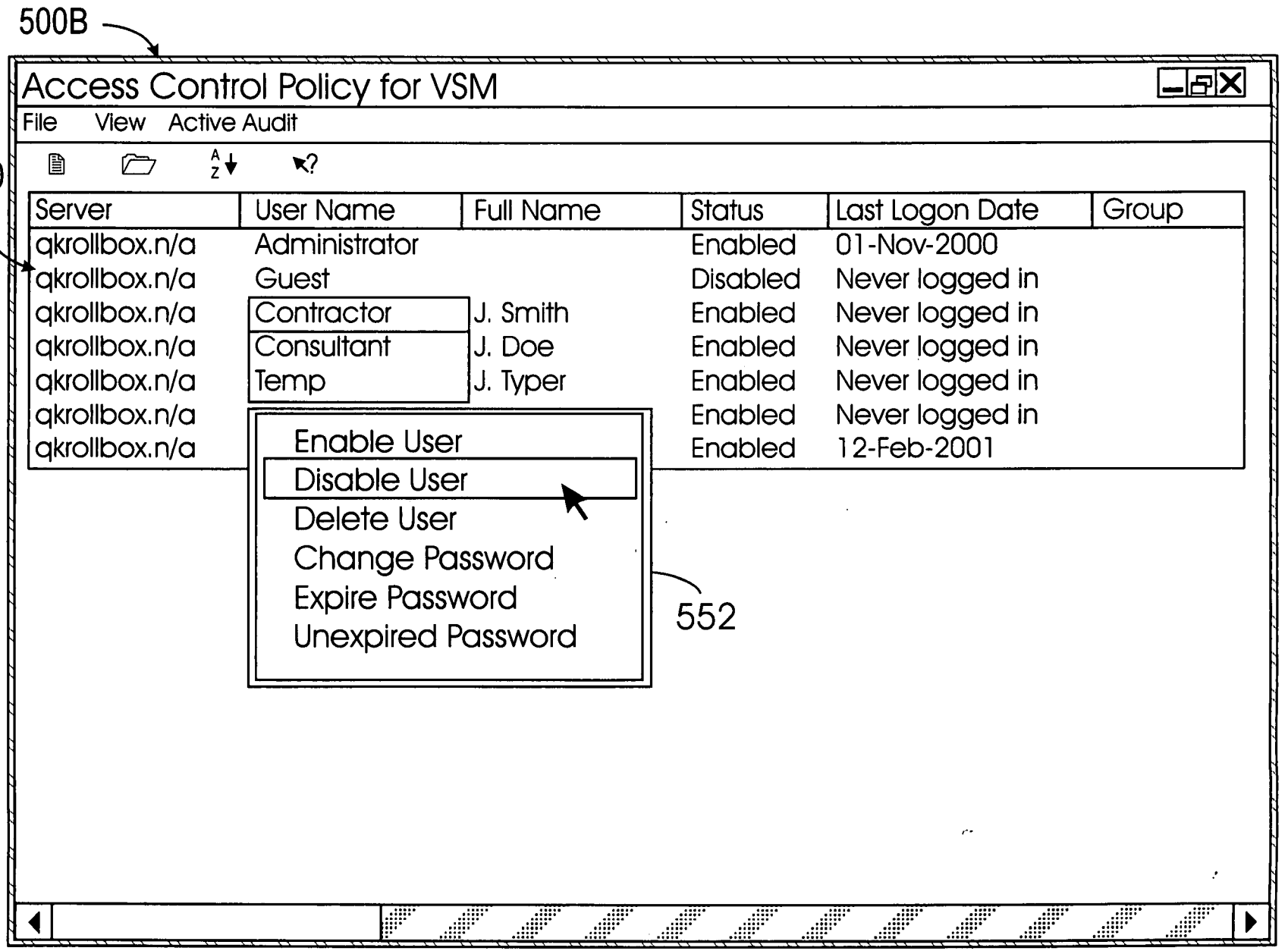

500B
Access Control Policy for VSM
File
View
Active Audit
550
Server
User Name
Full Name
Status
Last Logon Date
Group
qkrollbox.n/a
Administrator
Enabled
01-Nov-2000
qkrollbox.n/a
Guest
Disabled
Never logged in
qkrollbox.n/a
Contractor
J. Smith
Enabled
Never logged in
qkrollbox.n/a
Consultant
J. Doe
Enabled
Never logged in
qkrollbox.n/a
Temp
J. Typer
Enabled
Never logged in
qkrollbox.n/a
Enabled
Never logged in
qkrollbox.n/a
Enabled
12-Feb-2001
Enable User
Disable User
Delete User
Change Password
Expire Password
Unexpired Password
552

FIG. 13C

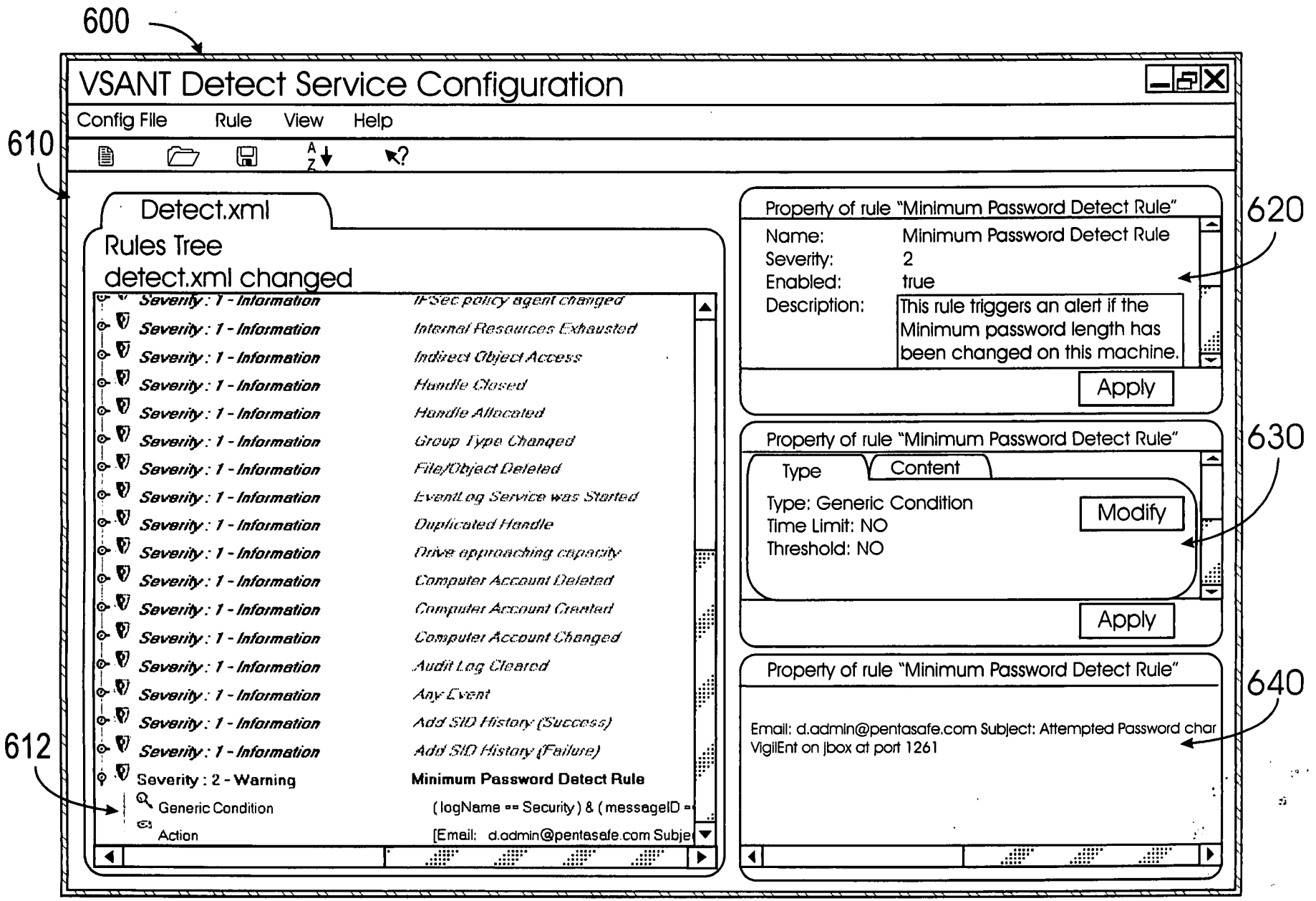

600
VSANT Detect Service Configuration
Config File
Rule
View
Help
610
Detect.xml
Rules Tree
detect.xml changed
Severity : 1 - Information
IPSec policy agent changed
Severity : 1 - Information
Internal Resources Exhausted
Severity : 1 - Information
Indirect Object Access
Severity : 1 - Information
Handle Closed
Severity : 1 - Information
Handle Allocated
Severity : 1 - Information
Group Type Changed
Severity : 1 - Information
File/Object Deleted
Severity : 1 - Information
EventLog Service was Started
Severity : 1 - Information
Duplicated Handle
Severity : 1 - Information
Drive approaching capacity
Severity : 1 - Information
Computer Account Deleted
Severity : 1 - Information
Computer Account Created
Severity : 1 - Information
Computer Account Changed
Severity : 1 - Information
Audit Log Cleared
Severity : 1 - Information
Any Event
Severity : 1 - Information
Add SID History (Success)
Severity : 1 - Information
Add SID History (Failure)
612
Severity : 2 - Warning
Minimum Password Detect Rule
Generic Condition
(logName == Security) & (messageID =
Action
[Email: d.admin@pentasafe.com Subje
Property of rule "Minimum Password Detect Rule"
620
Name: Minimum Password Detect Rule
Severity: 2
Enabled: true
Description: This rule triggers an alert if the Minimum password length has been changed on this machine.
Apply
Property of rule "Minimum Password Detect Rule"
630
Type
Content
Type: Generic Condition
Time Limit: NO
Threshold: NO
Modify
Apply
Property of rule "Minimum Password Detect Rule"
640
Email: d.admin@pentasafe.com Subject: Attempted Password char
VigilEnt on jbox at port 1261

FIG. 14